

COMPLETE PRACTICE TESTS

Provides **1200+ questions** covering all the exam objectives.



CompTIA Security+ SY0-701



by ExamsDigest®

CompTIA Security+ SY0-701 Practice Tests 2024®

Published by: ExamsDigest LLC. and LabsDigest LLC.

www.examsdigest.com - www.labsdigest.com Copyright © 2024

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher.

Trademarks: ExamsDigest, examsdigest.com and related trade dress are trademarks or registered trademarks of Examsdigest LLC. and may not be used without written permission. Amazon is a registered trademark of Amazon, Inc. All other trademarks are the property of their respective owners. ExamsDigest, LLC. is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE.

Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may find this material at [https://](https://examsdigest.com)

examsdigest.com

INTRODUCTION

The CompTIA Security+ SY0-701 examination is a global certification that validates the baseline skills you need to perform core security functions and pursue an IT security career.

About This Book

CompTIA Security+ SY0-701 Practice Tests 2024 by ExamsDigest is designed to be a practical practice exam guide that will help you prepare for the CompTIA Security+ SY0-701 exam.

This book has been designed to help you prepare for the style of questions you will receive on the CompTIA Security+ SY0-701 exam. It also helps you understand the topics you can expect to be tested on for each exam.

In order to properly prepare for the CompTIA Security+ SY0-701, I recommend that you:

✓ **Review a reference book:** CompTIA Security+ SY0-701 by Examsdigest is designed to give you sample questions to help you prepare for the style of questions you will receive on the real certification exam. However, it is not a reference book that teaches the concepts in detail. That said, I recommend that you review a reference book before attacking these questions so that the theory is fresh in your mind.

✓ **Get some practical, hands-on experience:** After you review the theory, I highly recommend getting your hands on using tools such

us packet tracer or GNS3. Also use the command-line tools from your OS to get a better understanding about ping, tracer, netstat and more commands. The more hands-on experience you have, the easier the exams will be.

✓ **Do practice test questions:** After you review a reference book and perform some hands-on work, attack the questions in this book to get you “exam ready”! Also claim your free 1-month access on our platform to dive into to more questions, flashcards and much much more.

Beyond The Book

This book gives you plenty of CompTIA Security+ SY0-701 questions to work on, but maybe you want to track your progress as you tackle the questions, or maybe you’re having trouble with certain types of questions and wish they were all presented in one place where you could methodically make your way through them. You’re in luck.

Your book purchase comes with a free one-month subscription to all practice questions online and more. You get on-the-go access any way you want it — from your computer, smartphone, or tablet. Track your progress and view personalized reports that show where you need to study the most. Study what, where, when, and how you want!

What you’ll find online

The online practice that comes free with this book offers you the same questions and answers that are available here and more.

The beauty of the online questions is that you can customize your online practice to focus on the topic areas that give you the most trouble.

So if you need help with the domain Network Security, then select questions related to this topic online and start practicing.

Whether you practice a few hundred problems in one sitting or a couple dozen, and whether you focus on a few types of problems or practice every type, the online program keeps track of the questions you get right and wrong so that you can monitor your progress and spend time studying exactly what you need.

You can access these online tools by sending an email to the info@examsdigest.com to claim access on our platform. Once we confirm the purchase you can enjoy your free access.

CompTIA Security+ SY0-701 Exam Details

The online practice that comes free with this book offers you the same questions and answers that are available here and more.

- ✓ **Format** - Multiple choice, multiple answer and performance-based
- ✓ **Type** - Associate
- ✓ **Delivery Method** - Testing center or online proctored exam
- ✓ **Time** - 90 minutes to complete the exam
- ✓ **Cost** - \$349
- ✓ **Language** - Available in English, Japanese

Exam Content

Content Outline

The CompTIA Security+ certification exam will verify the successful candidate has the knowledge and skills required to:

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions
- Monitor and secure hybrid environments, including cloud, mobile, and IoT
- Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance
- Identify, analyze, and respond to security events and incidents

The table below lists the domains measured by this examination and the extent to which they are represented:

1.0: General Security Concepts (12%)

2.0: Threats, Vulnerabilities, and Mitigations (22%)

3.0: Security Architecture (18%)

4.0: Security Operations (28%)

5.0: Security Program Management and Oversight (20%)

Table Of Content

Chapter 1 General Security Concepts	11
Questions 1-110	11
Answers 1-110	51
Chapter 2 Threats, Vulnerabilities, and Mitigations	164
Questions 111-220	164
Answers 111-220	204
Chapter 3 Implementation	322
Questions 221-310	322
Answers 221-310	355
Chapter 4 Security Operations	447
Questions 311-460	447
Answers 311-460	504
Chapter 5 Security Program Management and Oversight	659
Questions 461-540	659
Answers 461-540	689
Exam Simulator #1	772
Questions 1-100	772
Answers 1-100	808
Exam Simulator #2	914
Questions 101-200	914
Answers 101-200	950
Exam Simulator #3	1053
Questions 201-300	1053
Answers 201-300	1090
Exam Simulator #4	1198

Questions 301-400	1198
Answers 301-400	1234
Exam Simulator #5	1334
Questions 401-500	1335
Answers 401-500	1371
Exam Simulator #6	1474
Questions 501-600	1474
Answers 501-600	1513

CHAPTER 1

GENERAL SECURITY CONCEPTS

Questions 1-110

Question 1. A client disputes having signed a digital contract. The service provider needs to prove that the signature was indeed from the client and hasn't been tampered with. Which of the following security concepts is the service provider relying on?

- (A) Authentication
- (B) Confidentiality
- (C) Non-repudiation
- (D) Access Control

Question 2. Carlos, an IT consultant, advises a startup company on cybersecurity best practices. The company plans to launch several microsites under various subdomains. They want a solution that is cost-effective but also ensures that the sites are validated by a third-party. What type of certificate should Carlos recommend?

- (A) A separate self-signed certificate for each microsite
- (B) An individual third-party certificate for each subdomain
- (C) A third-party wildcard certificate
- (D) An EV certificate issued by an internal CA

Question 3. A company wants to ensure that security incidents are detected and addressed as quickly as possible by on-duty

personnel. Which of the following operational security controls would be BEST to implement for this purpose?

- (A) Deploying a Network Intrusion Prevention System (NIPS)
- (B) Establishing a 24/7 Security Operations Center (SOC)
- (C) Creating a company-wide security policy
- (D) Implementing end-to-end data encryption

Question 4. During a routine check, the IT department discovered that several employees had left their computers on and unattended during lunch break. Which operational security control can help mitigate the risk associated with this behavior?

- (A) Implementing biometric authentication
- (B) Enforcing a strict password policy
- (C) Deploying an automatic screen lock after inactivity
- (D) Implementing a secure coding practice

Question 5. An art gallery wants to deploy a security solution to detect movement in an open courtyard that features several sculptures. This space has varying temperature conditions, which might cause false alarms in some motion detection technologies. Which type of sensor would be MOST appropriate to ensure consistent motion detection in such conditions?

- (A) Thermal imaging sensors
- (B) Pressure-sensitive mats
- (C) Ultrasonic detectors
- (D) Microwave motion detectors

Question 6. A company's primary security control for accessing secure server rooms is a biometric fingerprint scanner.

However, the scanner occasionally malfunctions in high humidity. The security team is considering an alternative solution to grant access when the primary method fails. Which of the following would be the MOST appropriate compensating control?

- (A) Implementing a security token-based authentication system
- (B) Employing security guards at the main entrance
- (C) Installing security cameras inside the server room
- (D) Conducting regular server room audits

Question 7. A financial institution wants to ensure that customers are aware of the bank's policies on information sharing and how their personal data is used. Which of the following security controls would BEST communicate this to customers?

- (A) Implementing end-to-end encryption for online transactions
- (B) Publishing a privacy policy on the bank's website
- (C) Conducting annual cybersecurity awareness training for employees
- (D) Using multi-factor authentication for online banking

Question 8. A large financial organization wants to ensure that all employees understand the importance of cybersecurity and the role they play in safeguarding company assets. Which of the following managerial security controls will be MOST effective in achieving this?

- (A) Installing a firewall at the network perimeter
- (B) Regular security awareness training for employees

- (C) Deploying an Intrusion Detection System (IDS)
- (D) Encrypting all company data

Question 9. A company has faced multiple instances of unauthorized individuals gaining access to their office premises. Which of the following preventive security controls would be MOST effective in preventing unauthorized physical access?

- (A) Implementing a log monitoring solution for network traffic
- (B) Installing video surveillance cameras at all entry and exit points
- (C) Conducting regular security awareness training for employees
- (D) Implementing a multi-factor authentication system for network access.

Question 10. TechVault, a company specializing in secure storage solutions, recently had an unauthorized intrusion where a burglar managed to bypass their motion sensors. In a bid to prevent future breaches, they are considering deploying a system that can detect weight changes in a restricted floor area to alert any unauthorized access. Which of the following would be BEST for this requirement?

- (A) Ultrasonic motion detectors
- (B) Pressure-sensitive floor mats
- (C) CCTV cameras with facial recognition
- (D) Glass break sensors

Question 11. A system administrator is setting up an authentication system for a new web application. Which of the following security controls falls under the technical category

and ensures that users prove their identity before gaining access?

- (A) Implementing a security awareness training program
- (B) Conducting a background check for new employees
- (C) Using multi-factor authentication
- (D) Establishing a clean desk policy

Question 12. An e-commerce company has experienced a Distributed Denial of Service (DDoS) attack, which caused its website to become inaccessible for several hours. To mitigate the impact of such attacks in the future, which of the following would be the BEST corrective control to implement?

- (A) Displaying a seal for third-party security certifications on the website
- (B) Establishing a Web Application Firewall (WAF) with DDoS protection
- (C) Conducting routine vulnerability assessments on the website
- (D) Implementing strong password policies for website administrators

Question 13. GreenTech Industries has a manufacturing facility located in a relatively secluded area. Recent incidents of theft and trespassing have alarmed the management. Which of the following would MOST effectively deter unauthorized nighttime access to the perimeter of the facility?

- (A) Installing infrared sensors
- (B) Using bright perimeter lighting
- (C) Deploying additional security guards inside the facility
- (D) Increasing the height of the facility walls

Question 14. While conducting a routine security review, Jake, a security specialist, discovers an unexpected piece of data placed in the organization's financial system. Upon asking, he learns that this piece of data is intentionally placed and monitored to see if any unauthorized user or system interacts with it. What is this deceptive piece of data known as?

- (A) Honeystring
- (B) Honeytoken
- (C) Canary token
- (D) Security marker

Question 15. An organization is deploying new IoT devices in its smart office. To ensure that only authorized devices can connect to the corporate network, each device will be given a unique key pair. Which of the following best describes the system authentication approach the organization is using?

- (A) Shared secret authentication
- (B) Public key infrastructure (PKI)
- (C) Token-based authentication
- (D) Username and password authentication

Question 16. In the new branch of BankSecure, the management has decided to install a security system at the main entrance that forces visitors to go through two separate authorization checks before entering the main premises. Which physical security measure should they consider?

- (A) Turnstiles
- (B) Security Guards
- (C) Access Control Vestibule
- (D) Keycard Readers

Question 17. The IT department wants to monitor network traffic in real time to detect any anomalies or malicious activities. Which of the following security controls can accomplish this?

- (A) Security policy documentation
- (B) Intrusion Detection System (IDS)
- (C) Employee code of conduct
- (D) Access Control Lists (ACL)

Question 18. Jenna, a web administrator for a growing online retail business, is in the process of obtaining SSL certificates for the company's domain. The company uses several subdomains for different services, such as shop.example.com, blog.example.com, and support.example.com. Instead of obtaining individual certificates for each subdomain, Jenna wants to use one certificate. What type of certificate should Jenna pursue?

- (A) Extended Validation Certificate
- (B) Wildcard Certificate
- (C) Certificate with Subject Alternative Names (SAN)
- (D) Code Signing Certificate

Question 19. At a newly established museum, management wants to install sensors in the exhibit rooms to detect any unauthorized movement after hours. The rooms are often filled with a mix of air conditioning and external noise from the city. Which sensor would be BEST suited to detect movement in such conditions without being affected by the noise?

- (A) Acoustic sensors
- (B) Glass break detectors

- (C) Ultrasonic sensors
- (D) Thermal imaging cameras

Question 20. A company is setting up a secure communication channel between its headquarters and a remote branch office. To ensure that data transmitted over this channel originates from a legitimate system at the branch office, the company is considering using digital certificates. Which authentication method for systems is the company contemplating?

- (A) Kerberos authentication
- (B) Password-based authentication
- (C) Certificate-based authentication
- (D) Biometric-based authentication

Question 21. A financial institution has experienced an uptick in unauthorized transactions. They want to implement a control that will allow them to identify suspicious transactions in real-time. Which of the following would be the BEST detective control for this scenario?

- (A) Implementing a multi-factor authentication system for all users
- (B) Establishing a Security Operations Center (SOC) to monitor network traffic
- (C) Installing an Intrusion Detection System (IDS) on their network
- (D) Restricting transaction capabilities to only a few trusted IP addresses.

Question 22. TechHaus has recently experienced multiple security breaches where unauthorized personnel have managed to infiltrate their server rooms after hours. To enhance security

measures, the company decided to deploy a new system. Which of the following options would BEST detect human intruders based on their body heat even in complete darkness?

- (A) Installing CCTV cameras with LED lights
- (B) Using ultrasonic motion sensors
- (C) Deploying infrared (IR) sensors
- (D) Implementing RFID badge readers at the entrance

Question 23. After detecting an unauthorized intrusion into their network, a financial institution wants to implement a control that will restore compromised systems to a known good state. Which of the following would be the MOST appropriate corrective control?

- (A) Implementing Intrusion Detection Systems (IDS) across the network
- (B) Frequently updating firewall rules
- (C) Restoring systems from verified backups
- (D) Enabling multi-factor authentication for users

Question 24. After a recent security breach, Sarah, a cybersecurity analyst, is implementing additional measures to detect unauthorized activities. She decides to embed specific values in the database that serve no real purpose but are monitored for any unauthorized access or usage. These values are designed to raise alerts if they are ever accessed or used. What are these specific values commonly referred to as?

- (A) Security flags
- (B) Honeypots
- (C) Honeytokens
- (D) Audit trails

Question 25. Bob receives an email prompting him to verify his identity by clicking on a link. The link directs him to a webpage where he has to provide his username, password, and answer a personal security question. What type of authentication method is being employed here?

- (A) Biometric authentication
- (B) Token-based authentication
- (C) Two-factor authentication
- (D) Single sign-on

Question 26. In an effort to minimize data breaches from malware, a company is deciding on a control to prevent malicious software from being executed on company devices. Which of the following would be the BEST preventive control?

- (A) Deploying a Network Intrusion Detection System (NIDS)
- (B) Regularly backing up critical data
- (C) Installing an antivirus software with real-time scanning
- (D) Performing a forensic analysis after a security incident

Question 27. After undergoing a major infrastructure upgrade, GlobalMed Corp experienced several unanticipated security issues. In retrospect, the IT manager realized they skipped an essential step in their change management process which could have predicted and mitigated these issues. What step did they most likely overlook?

- (A) Procurement of new hardware
- (B) Training of IT staff on the new systems
- (C) Impact analysis
- (D) Integration with legacy systems

Question 28. MegaCorp recently introduced a new web application for its customers. Before its release, the software underwent rigorous testing in a controlled environment. When the application was deployed in production, several security vulnerabilities were reported. Which of the following reasons can explain the mismatch between the test results and actual vulnerabilities?

- (A) The testing environment was an exact replica of the production environment
- (B) Test results were not thoroughly reviewed
- (C) The software was not tested for zero-day vulnerabilities
- (D) Penetration testing was done post-production

Question 29. An online banking website employs a system that automatically logs out users after 10 minutes of inactivity to ensure that if a user forgets to log out, no one else can alter the user's banking details. Which principle of the CIA triad is the banking website MOST directly addressing?

- (A) Confidentiality
- (B) Availability
- (C) Authentication
- (D) Integrity

Question 30. A company is located in an area prone to natural disasters such as earthquakes and floods. Which of the following physical security controls would be MOST effective in ensuring the safety of the company's IT infrastructure?

- (A) Using biometric authentication for server access
- (B) Deploying a firewall to protect against cyber threats
- (C) Establishing a raised floor system in the data center
- (D) Conducting penetration testing on a regular basis

Question 31. TechBank has just opened a new branch in the city center. Due to its location, the management is concerned about potential vehicular attacks on the facility. Which of the following physical security measures can TechBank employ to specifically deter such attacks?

- (A) Surveillance Cameras
- (B) Bollards
- (C) Access Badges
- (D) Security Guards

Question 32. During a security assessment, Maria, a security consultant, identifies a self-signed certificate being used on a client's public-facing web server. What is the PRIMARY security concern related to this finding?

- (A) The web server might be vulnerable to Distributed Denial of Service (DDoS) attacks
- (B) The certificate could be expired
- (C) Users cannot validate the authenticity of the website easily
- (D) The web server might not support modern encryption algorithms

Question 33. TechFin Bank is considering implementing a new software system for their transaction processing. Before rolling it out, the cybersecurity team insists on carrying out a specific type of analysis to understand how this change might affect the organization's security posture. What is the team referring to?

- (A) Risk appetite assessment
- (B) Performance benchmarking
- (C) Impact analysis
- (D) Penetration testing

Question 34. To discourage potential cybercriminals from targeting their online storefront, an e-commerce company is considering various security measures. Which of the following would act MOST effectively as a deterrent control?

- (A) Displaying a seal for third-party security certifications on the website
- (B) Using a Web Application Firewall (WAF)
- (C) Conducting monthly vulnerability assessments
- (D) Storing customer data in encrypted databases

Question 35. The security team of a multinational company deployed a network of honeypots globally, making it appear as an interconnected and realistic environment. They aim to study coordinated multi-stage attacks. This deceptive setup is known as:

- (A) Firewall Cluster
- (B) Virtual LAN (VLAN)
- (C) Distributed Denial of Service (DDoS) Prevention
- (D) Honeynet

Question 36. ExamsDigest Corp, a technology company, recently conducted a security assessment to align with industry best practices. The company's current security posture was compared to its desired future state, revealing discrepancies. Which of the following best describes the approach ExamsDigest Corp employed?

- (A) Vulnerability Assessment
- (B) Penetration Testing
- (C) Gap Analysis
- (D) Threat Modeling

Question 37. A pharmaceutical company is concerned about competitors accessing their formula for a new drug. Which pillar of the CIA triad is MOST directly addressed by their concern?

- (A) Availability
- (B) Confidentiality
- (C) Integrity
- (D) Non-repudiation

Question 38. FinCorp, a financial institution, has recently adopted a new security framework. In this framework, every device and user inside the organization's network is treated as if they were outside the perimeter, necessitating rigorous verification processes even for internal requests. Which security paradigm has FinCorp implemented?

- (A) Demilitarized Zone (DMZ)
- (B) Network Segmentation
- (C) Intrusion Detection System (IDS)
- (D) Zero Trust

Question 39. GreenValley Mall, located in a busy urban area, has recently faced security concerns due to the proximity of its main entrance to a major road. Which physical security enhancement can the mall management implement to create a protective barrier between the road and the entrance, ensuring pedestrian safety and preventing unauthorized vehicular access?

- (A) Reinforced Walls
- (B) Metal Detectors
- (C) Bollards
- (D) Perimeter Fencing

Question 40. A tech company, InnovateTech, has recently faced multiple incidents of unauthorized personnel trying to access their R&D labs. They wish to monitor and record all activities near the entrance of this sensitive area. Which physical security measure would be most effective for this requirement?

- (A) RFID Badge Readers
- (B) Biometric Scanners
- (C) Video Surveillance Cameras
- (D) Mantrap

Question 41. A cybersecurity analyst at XYZ Corp is looking to deploy a system that appears to be vulnerable and enticing to attackers. The main goal is to study the tactics, techniques, and procedures (TTPs) of potential adversaries, without them realizing that they're interacting with a decoy. Which of the following would BEST meet this requirement?

- (A) Intrusion Detection System (IDS)
- (B) Firewall
- (C) Honeypot
- (D) VPN Concentrator

Question 42. A multinational organization recently experienced a significant security breach. After investigating, it was determined that a change to the network infrastructure was made without undergoing the standard approval process. As a result, there was a misconfiguration which allowed unauthorized access. What security principle related to change management did the organization neglect?

- (A) Configuration baseline reviews
- (B) Least privilege enforcement

- (C) Approval process adherence
- (D) Patch management

Question 43. After a series of cyber-attacks on a company's infrastructure, the IT team decided to deploy a solution that would seem like a legitimate part of their network but is intentionally isolated and monitored. They intend to detect and analyze malicious activities in this isolated environment. What technology are they most likely implementing?

- (A) Network segmentation
- (B) Honeypot
- (C) DMZ (Demilitarized Zone)
- (D) Sandboxing

Question 44. Liam, the CTO of a medium-sized enterprise, noticed that several software applications were not updated regularly, leading to potential security vulnerabilities. Upon investigation, he realized that no specific team or individual was assigned as the owner of these applications. To enhance security, what should Liam emphasize?

- (A) Immediate decommissioning of all unowned applications
- (B) Assignment of clear ownership to all business applications
- (C) Conducting monthly vulnerability assessments on all applications
- (D) Outsourcing the management of these applications to third-party vendors

Question 45. TechSoft Corp, a mid-sized software development firm, is relocating its main office to a new building. The

management is concerned about potential threats after hours, particularly due to the increasing reports of cyber-espionage. They are evaluating different security measures. Which option would provide an immediate physical presence and deterrence during non-business hours?

- (A) CCTV with motion detection
- (B) Retinal scan at all entrances
- (C) Security guard presence
- (D) Reinforced doors and windows

Question 46. Alice, a system administrator for a startup, is preparing to deploy a new website for her company. To ensure secure communications between the users and the website, she plans to obtain a digital certificate for the site. Before doing so, which step must Alice first undertake to get a certificate from a Certificate Authority (CA)?

- (A) Generate a public-private key pair
- (B) Submit her passport copy to the CA
- (C) Download the latest CA root certificate
- (D) Encrypt the website with symmetric encryption

Question 47. Julia, a security administrator, is concerned about potential unauthorized access to confidential project files stored on a company server. She decides to place a document within the project folders that seems enticing but is actually monitored for access. This strategy aims to detect if someone is accessing files without authorization. What is this document commonly known as?

- (A) Salt file
- (B) Honeyfile

- (C) Log file
- (D) Backup file

Question 48. After a recent incident of vandalism, a corporate building is considering implementing security controls that would dissuade potential perpetrators. Which of the following would serve BEST as a deterrent control?

- (A) Encrypting all stored data
- (B) Installing biometric access controls on all entrances
- (C) Implementing regular data backups
- (D) Placing visible security signage indicating 24/7 surveillance

Question 49. Alice wants to access a restricted online portal. The portal asks her to enter a unique username and a secret passphrase only she should know. This process helps the system ensure that Alice is who she claims to be. What security concept is the portal employing?

- (A) Authorization
- (B) Accounting
- (C) Multifactor authentication
- (D) Authentication

Question 50. Sophia, the cybersecurity lead at XYZ Corp, is in the process of drafting a new security policy. During the drafting process, she primarily consults with her security team. However, upon implementation, several departments pushed back due to the policy interfering with their operations. Which best describes the misstep Sophia made during the policy creation process?

- (A) Not using a standardized security framework

- (B) Over-reliance on automated security solutions
- (C) Not including key stakeholders in the policy drafting process
- (D) Focusing too much on external threats rather than internal ones

Question 51. BioGen Inc., a biotechnology company, has implemented a layered security approach. They are considering adding a human element to their security measures for their research labs. Which of the following would best provide the ability to evaluate and respond to various security situations with human judgment?

- (A) Installing biometric locks
- (B) Employing security guards
- (C) Implementing an access control vestibule
- (D) Deploying AI-driven security cameras

Question 52. While analyzing server logs, Mike, an IT security analyst, noticed that an unfamiliar document was frequently accessed. Upon investigation, he realized that this document was deliberately placed by the security team and had no real data but was closely monitored. The purpose of this file is MOST likely:

- (A) To serve as a redundancy copy in case of data loss
- (B) To act as a decoy to attract and detect unauthorized access
- (C) To maintain a record of all user activities for auditing
- (D) To be encrypted and sent to clients as a sample

Question 53. DataCenter Inc. is located in a region prone to protests and vandalism. They wish to enhance their perimeter

security to deter potential intruders and make it visibly clear that unauthorized access is restricted. Which of the following physical security measures would be the most effective first line of defense for the company?

- (A) Sliding Doors
- (B) Security Cameras
- (C) High-security Fencing
- (D) Proximity Card Readers

Question 54. SecureTech Corp, a company dealing with sensitive client data, is redesigning its main office entrance to enhance security. They want to ensure that only one person gains access at a time, even if multiple people try to enter using a single authorized access badge. Which of the following would best serve this purpose?

- (A) CCTV Cameras
- (B) Mantrap
- (C) Biometric Scanners
- (D) Motion Detectors

Question 55. While setting up a new internal web application, Laura, a system administrator, decides to use a digital certificate for SSL/TLS encryption. Due to budget constraints, she can't procure a certificate from a commercial Certificate Authority (CA). Which of the following would be a viable option for Laura to secure the application?

- (A) Rely on plaintext HTTP for the application
- (B) Obtain a certificate from a free Certificate Authority
- (C) Generate a self-signed certificate
- (D) Use a shared certificate from another application

Question 56. A network administrator has received a new security patch for a mission-critical application. Which of the following is the BEST action to take before applying this patch in the live environment?

- (A) Apply the patch immediately to ensure system security
- (B) Notify all users about the upcoming downtime due to the patch
- (C) Test the patch in a separate testing environment
- (D) Take a backup of only the mission-critical application

Question 57. After implementing a major security update to its database system, TechCo experienced unexpected downtime and system incompatibilities. The CISO wants to ensure that such incidents can be quickly addressed in the future. Which of the following should TechCo have had in place before deploying the update to mitigate the impact of these kinds of incidents?

- (A) A comprehensive list of all updates
- (B) An automated system recovery tool
- (C) A backout plan
- (D) A detailed user manual for the update

Question 58. A financial institution processes thousands of credit card transactions daily. To ensure the security and integrity of these transactions, the security officer wants to employ a solution that will safely manage and store cryptographic keys. Which of the following would be the MOST suitable solution?

- (A) Trusted Platform Module (TPM)
- (B) Full Disk Encryption (FDE)

- (C) Hardware Security Module (HSM)
- (D) Software Key Repository

Question 59. During the setup of a secure communication channel, Alice and Bob need to agree upon a shared secret key without sending the key directly to each other, as they fear eavesdropping. Which protocol would best facilitate this requirement?

- (A) RSA
- (B) HMAC
- (C) Diffie-Hellman
- (D) AES

Question 60. A company is developing a new video conferencing tool. They want to make sure that all video and audio data transmitted between participants are encrypted and protected from eavesdropping. Which type of encryption should the developers implement to achieve this?

- (A) Endpoint Encryption
- (B) Transport-layer Encryption
- (C) Volume-level Encryption
- (D) Database-level EncryptionAccess Control

Question 61. After a significant cybersecurity incident, ABC Tech revamped its incident response procedures. However, the documentation was not updated to reflect these changes. During a subsequent minor incident, there was confusion regarding the steps to be followed. Which of the following is the MOST direct implication of not updating the incident response documentation?

- (A) The company may have to invest in new cybersecurity

tools

- (B) Stakeholders might lose trust in the company's ability to handle incidents
- (C) Incident response might be inconsistent and less effective
- (D) ABC Tech may have to hire external consultants for incident response

Question 62. A financial organization is considering implementing a system that allows all users to view all transactions, but once a transaction is recorded, it cannot be altered or deleted. They want this transparency to foster trust among their users. Which of the following would best meet this requirement?

- (A) Digital certificate
- (B) Open public ledger
- (C) Symmetric encryption
- (D) Secure file transfer protocol

Question 63. A company is implementing a system to ensure that code released to production is both unaltered and approved by a specific team member. Which of the following cryptographic techniques should they implement?

- (A) Symmetric encryption of the code
- (B) Hashing the code with SHA-256
- (C) Encrypting the code with the team member's public key
- (D) Digital signature by the team member

Question 64. Your company has recently deployed an update to its CRM application. Post-update, users are experiencing connectivity issues. As a security administrator, which of the

following steps should you take FIRST to address the connectivity problem without causing data loss?

- (A) Restart the application immediately
- (B) Disconnect all users and then restart the application
- (C) Validate the update's integrity and then restart the application
- (D) Reinstall the previous version of the CRM application

Question 65. TechDynamics, a growing tech startup, plans to scale its operations and serve a global clientele. Given that their client base operates in multiple time zones, when should TechDynamics schedule their system maintenance to ensure minimal disruption?

- (A) During the busiest hours for their headquarters' local time
- (B) Staggered based on the peak hours of their global clients
- (C) Only when a system breakdown occurs
- (D) Establish a consistent maintenance window during off-peak hours for the majority of their clientele

Question 66. During an IT audit, a company's encryption practices come under scrutiny. The IT auditor recommends increasing the encryption key length for certain applications to improve security. What is the PRIMARY reason to increase the encryption key length?

- (A) To speed up encryption and decryption processes
- (B) To ensure compatibility with older systems
- (C) To reduce the possibility of a brute force attack
- (D) To reduce the key management overhead

Question 67. Sarah is working on a project where she needs to validate the integrity and authenticity of assets over time, without a centralized authority. Which technology would be most appropriate for this use case?

- (A) Digital signature
- (B) Key escrow
- (C) Blockchain
- (D) Key management system

Question 68. A graphic design company frequently works with large files such as videos and high-resolution images. These files are stored on a dedicated storage volume in their server. While they need to secure this data, they don't want to encrypt individual files due to the volume of data and frequent access needs. Which encryption approach is most appropriate for this scenario?

- (A) File-level Encryption
- (B) Full-disk Encryption
- (C) Transport-layer Encryption
- (D) Volume-level Encryption

Question 69. An e-commerce company stores millions of customer transaction records in their primary database. They have decided to enhance their security posture by applying encryption to protect sensitive data. However, they don't want to encrypt the entire server storage, just the data within the database. Which encryption approach should the company adopt to meet their objective?

- (A) Full-disk Encryption
- (B) File-level Encryption

- (C) Volume-level Encryption
- (D) Database-level Encryption

Question 70. Your organization plans to upgrade its database system. To maintain security during this process, which of the following actions should be RESTRICTED until the upgrade is validated?

- (A) Monitoring the database for any anomalies
- (B) Allowing end-users to access the upgraded database
- (C) Making regular backups of the database
- (D) Reviewing the database system logs

Question 71. A journalist wants to send a confidential message to her editor without raising suspicion. Instead of sending a coded or encrypted text, she embeds the message within a harmless-looking photograph. What method is she employing to keep the message concealed?

- (A) Digital signature
- (B) Tunneling
- (C) Steganography
- (D) Chaining

Question 72. A security administrator needs to apply a configuration change to a critical service, requiring a service restart. Before initiating the restart, which of the following steps is MOST important to ensure continuous service availability?

- (A) Implement automatic service restart on failure
- (B) Announce the restart to all company employees
- (C) Schedule the restart during off-peak hours
- (D) Take a backup of the current service configuration

Question 73. A security analyst at DataCorp is tasked with preventing unauthorized external applications from connecting to their server. Which approach should the analyst primarily rely on to achieve this?

- (A) Implement an allow list for approved applications
- (B) Monitor server CPU usage
- (C) Regularly patch server software
- (D) Encrypt data at rest on the server

Question 74. Alice needs to provide proof of the authenticity of a digital document she's sending to Bob. Which of the following cryptographic elements should Alice use to accomplish this task and ensure Bob knows the document came from her?

- (A) Encrypt the document with Bob's private key
- (B) Encrypt the document with her public key
- (C) Sign the document with her private key
- (D) Sign the document with Bob's public key

Question 75. Carla, a security analyst, receives an alert that one of the company's server certificates may have been exposed in a recent data breach. What is the most immediate action Carla should take to ensure that the exposed certificate cannot be used maliciously?

- (A) Request a new certificate from the CA
- (B) Update the company firewall rules
- (C) Add the certificate to the Certificate revocation list (CRL)
- (D) Perform a vulnerability assessment on the server

Question 76. A database administrator is concerned about identical hashes being produced for users who select the same password. To mitigate this risk, what cryptographic technique should the administrator implement?

- (A) Digital signature
- (B) Salting
- (C) Key stretching
- (D) Symmetric encryption

Question 77. An online retailer is considering various methods to protect its customers' credit card information. Instead of storing the actual credit card numbers in their database, they opt for a solution that replaces the numbers with unrelated, random values. What is this method called?

- (A) Symmetric encryption
- (B) Digital watermarking
- (C) Hashing
- (D) Tokenization

Question 78. During a scheduled maintenance window, a security administrator plans to apply a critical update to the company's firewall. Which of the following actions is MOST crucial to ensure minimized downtime during this process?

- (A) Notifying the firewall vendor about the update
- (B) Disabling all firewall rules temporarily
- (C) Creating a rollback plan in case of update failure
- (D) Scheduling the update during peak business hours

Question 79. A security administrator is considering a cryptographic solution for protecting data in transit between two servers located in the same data center. The primary goal is to

ensure speed and efficiency in encryption and decryption processes. Which type of encryption would best meet this requirement?

- (A) Asymmetric encryption using RSA
- (B) Symmetric encryption using AES
- (C) Hybrid encryption using a combination of RSA and AES
- (D) Asymmetric encryption using ECC

Question 80. A software developer wants to store user passwords in a way that even if the database is compromised, attackers would not be able to retrieve the original passwords. What technique should the developer use to achieve this?

- (A) Symmetric encryption
- (B) Digital signing
- (C) Hashing
- (D) Steganography

Question 81. A software development company is working on a mobile banking application. They want to ensure that sensitive operations like cryptographic processes and biometric data validation are isolated from the main operating system to prevent potential tampering. Which tool should they consider implementing to achieve this objective?

- (A) Hardware Security Module (HSM)
- (B) Key Management System (KMS)
- (C) Secure enclave
- (D) Trusted Platform Module (TPM)

Question 82. A web server hosting the company's e-commerce site is set for an OS upgrade. The upgrade is expected to last 30

minutes. What should be a primary consideration to minimize customer impact due to potential downtime?

- (A) Implementing a load balancer
- (B) Taking a backup of the e-commerce site
- (C) Posting a maintenance notice a week in advance
- (D) Upgrading the server's hardware

Question 83. A project manager is working on a new product launch and has documents with sensitive financial projections on her local computer. She occasionally shares these documents with select board members via email. While she wants to keep the financial documents secure, she doesn't want to encrypt all the data on her computer. Which encryption approach should she utilize?

- (A) Full-disk Encryption
- (B) Transport-layer Encryption
- (C) File-level Encryption
- (D) Partition Encryption

Question 84. A security analyst is evaluating security enhancements for a series of laptops that will store highly confidential data. The analyst wants to ensure that stored data remains encrypted and the integrity of the boot process is maintained. Which of the following would BEST meet this requirement?

- (A) Installing antivirus software on each laptop
- (B) Enabling a software-based full-disk encryption
- (C) Implementing a BIOS password
- (D) Utilizing a Trusted Platform Module (TPM)

Question 85. A large e-commerce company is deploying a new online payment system. The Chief Information Security Officer (CISO) is concerned about the security of cryptographic keys and wants to ensure they are protected from potential theft or compromise. Which tool should the CISO implement to provide the HIGHEST level of security for these keys?

- (A) Password vault
- (B) Software-based key storage
- (C) Hardware Security Module (HSM)
- (D) Cloud-based encryption service

Question 86. Sarah, a security analyst, is concerned about potential man-in-the-middle attacks on the company's internal portal. To mitigate this risk, she recommends obtaining a digital certificate from a trusted entity. Which of the following is responsible for issuing such certificates?

- (A) Key distribution center
- (B) Certificate authority (CA)
- (C) Tokenization system
- (D) Security incident event manager

Question 87. A financial institution is looking to adopt an encryption algorithm for its transactions that is considered to be very secure due to its longer key length, compared to older standards. Which encryption algorithm best fits this description?

- (A) DES
- (B) Blowfish
- (C) RSA
- (D) AES-256

Question 88. Alice receives an email from Bob with an attached document. She wants to verify both the authenticity of the sender and the integrity of the attached document. Which of the following should Bob have used before sending the email?

- (A) Encrypt the document with his private key
- (B) Hash the document
- (C) Encrypt the document with Alice's public key
- (D) Sign the document with his private key

Question 89. During a critical financial quarter, GlobalFin Corp experienced unexpected outages during peak business hours due to system maintenance, impacting its operations significantly. To prevent such occurrences in the future, what should GlobalFin Corp implement regarding their maintenance activities?

- (A) Conduct maintenance activities randomly to avoid predictability
- (B) Implement maintenance activities during peak business hours
- (C) Establish designated maintenance windows
- (D) Reduce the frequency of maintenance activities

Question 90. A financial institution wants to securely transfer transaction data between its main office and a branch office. The data should be encrypted while in transit to prevent any interception and unauthorized access. Which encryption solution is most suitable for securing the data during transport?

- (A) Database-level Encryption
- (B) Full-disk Encryption
- (C) Transport-layer Encryption
- (D) File-level Encryption

Question 91. After a recent software update, a company's intranet portal has been inaccessible to a few employees. The IT team suspects it could be due to network filtering rules. What should the IT team review to confirm their suspicions?

- (A) The content filtering policies
- (B) The malware detection logs
- (C) The allow list/deny list configurations
- (D) The network bandwidth utilization graphs

Question 92. A user wants to send a confidential email to their colleague and ensure that only the intended recipient can read it. The user also wants to provide assurance to the recipient that the email was indeed sent by them. Which encryption method should the user employ to accomplish this?

- (A) Use symmetric encryption with a shared key
- (B) Use asymmetric encryption and encrypt the email with the recipient's public key
- (C) Use asymmetric encryption, encrypt the email with the user's private key
- (D) Use asymmetric encryption, first sign the email with the user's private key, then encrypt it with the recipient's public key

Question 93. A user, Amy, wants to securely send a confidential document to her colleague, Bob. Amy decides to encrypt the document to ensure its confidentiality. Which of the following should Amy use to encrypt the document, ensuring only Bob can decrypt it?

- (A) Amy's private key
- (B) Amy's public key
- (C) Bob's private key
- (D) Bob's public key

Question 94. A cybersecurity analyst is investigating a suspicious image file received via email. Upon closer examination, the analyst suspects that the image might be carrying hidden data because the file size is unusually large. Which technique might the sender have used to embed secret information within the image?

- (A) Symmetric encryption
- (B) Digital watermarking
- (C) Steganography
- (D) Hashing

Question 95. A company is preparing to roll out a new infrastructure deployment for its internal network. They have a server that will store both highly confidential customer information and non-sensitive marketing material. The IT department wants to ensure that only the confidential data is encrypted, while the marketing data remains easily accessible. Which level of encryption would be most suitable for this scenario?

- (A) File-level Encryption
- (B) Full-disk Encryption
- (C) Partition Encryption
- (D) Transport-layer Encryption

Question 96. Sarah, a cybersecurity analyst, receives a report that a company laptop was stolen from an employee's car. The laptop contained sensitive financial data. Sarah checked the company's security configurations and found that the laptop was equipped with full-disk encryption. How does this impact the potential data breach situation?

- (A) The data remains easily accessible, as only the boot

sector was encrypted

- (B) The data is protected, as the entire hard drive's contents are encrypted
- (C) The data is partially encrypted, with only the user directories protected
- (D) The data is vulnerable since full-disk encryption only applies when the laptop is connected to the company network

Question 97. A university's IT department provides access to its student records for training purposes to new hires. To protect student identities, they replace the real names and social security numbers with fictitious ones while maintaining the database's original format. Which technique is the IT department utilizing?

- (A) Digital signing
- (B) Data masking
- (C) Steganography
- (D) Data deduplication

Question 98. A company is looking for a cryptographic solution that provides an immutable and transparent record of all transactions in a distributed ledger system. Which of the following would BEST meet this requirement?

- (A) Symmetric key algorithm
- (B) Public key infrastructure
- (C) Blockchain
- (D) Digital watermark

Question 99. An IT manager is considering solutions to protect data stored on the laptops provided to remote employees. The primary concern is to ensure that the entire content of the

laptop's storage drive is unreadable if a laptop is lost or stolen. Which encryption level would best address this concern?

- (A) File-level Encryption
- (B) Transport-layer Encryption
- (C) Full-disk Encryption
- (D) Database-level Encryption

Question 100. The finance department at a large firm still relies on a legacy application for their quarterly reporting. This application is known to have some security flaws, but due to its critical nature, it cannot be easily replaced. How can the firm BEST mitigate the risks associated with this application?

- (A) Train the finance team about the latest cybersecurity threats
- (B) Run the legacy application on the latest hardware to improve performance
- (C) Place the legacy application behind a web application firewall (WAF)
- (D) Frequently change the passwords of users who have access to the application

Question 101. A multinational corporation is concerned about the possibility of losing access to encrypted data due to the loss or compromise of private keys. They've approached a third-party organization for a solution. Which of the following is a system that allows the third party to securely hold a copy of the corporation's cryptographic keys to ensure data recoverability?

- (A) Public Key Repository
- (B) Key Generation Center
- (C) Key Escrow
- (D) Key Renewal Service

Question 102. A financial institution plans to provide access to its database for third-party developers to create new applications. However, they want to ensure that the developers do not see the actual data but instead work with a disguised version that retains the data's original structure. What technique is the financial institution considering?

- (A) Tokenization
- (B) Data masking
- (C) Encryption
- (D) Digital watermarking

Question 103. NexTech, a cloud-based software company, recently faced a security breach due to inconsistent practices among its system administrators. To avoid such inconsistencies in the future, what should NexTech emphasize in its operations?

- (A) Rely on system administrators to develop their personal methods
- (B) Mandate frequent system reboots
- (C) Implement Standard Operating Procedures (SOPs) for all technical operations
- (D) Conduct random security audits without notifying administrators

Question 104. After a series of system enhancements, a financial organization decided to use a manual method of documenting changes in separate files rather than implementing a version control system. During an audit, the cybersecurity team struggled to determine which version of a critical system file was the most recent and accurate. What is the PRIMARY risk of not implementing version control for such documentation?

- (A) Increased storage requirements for multiple files
- (B) Difficulty in collaborating between team members
- (C) Lack of traceability and difficulty in reverting to a known stable state
- (D) Greater need for training staff on manual documentation

Question 105. During a security audit, it was found that an application was using plain hashes for storing passwords. The security team recommended a method that involves using the original password along with a salt and then rehashing it multiple times. What is this method known as?

- (A) Key clustering
- (B) Rainbow table prevention
- (C) Key rotation
- (D) Key stretching

Question 106. During a routine update, a web server application requires a restart. What should the administrator do FIRST to ensure client connections aren't abruptly terminated during the restart?

- (A) Redirect incoming traffic to a backup server
- (B) Increase the server's memory
- (C) Manually terminate all active client sessions
- (D) Check for available patches for the application

Question 107. Carlos is responsible for managing IT services for a university. The university has numerous departments, each with its subdomain, like arts.university.com, science.university.com, and sports.university.com. Carlos wants a solution that ensures HTTPS security while being cost-effective. However, he's wary of potential risks. What might be

a drawback of using a Wildcard Certificate for the university's subdomains?

- (A) It can secure only one subdomain
- (B) If compromised, all subdomains are at risk
- (C) It only validates the domain ownership, not the organization's identity
- (D) It's the most expensive certificate available

Question 108. Your organization is preparing to upgrade a database server that supports an e-commerce application. A review of the change management documentation has revealed that multiple applications rely on this particular database server for various functionalities. Which of the following steps should be taken FIRST to ensure a smooth upgrade process without disruptions?

- (A) Upgrade the database server immediately to benefit from new features
- (B) Perform a backup of the database server
- (C) Identify and test all applications that have dependencies on the database server
- (D) Inform users about potential downtime during the upgrade

Question 109. After a recent data breach, a multinational corporation is evaluating its cryptographic practices. The Chief Security Officer (CSO) determines that the manual management of cryptographic keys has become too complex due to the scale of the operations. Which tool would BEST address the CSO's concern while ensuring robust security practices?

- (A) Password Management System
- (B) Secure File Transfer Protocol (SFTP)

- (C) Trusted Platform Module (TPM)
- (D) Key Management System (KMS)

Question 110. During a quarterly review, the IT team at a logistics company decided to change the configuration of their load balancers to better distribute traffic among their servers. After the change, a series of technical issues emerged, affecting customer-facing applications. When troubleshooting the issue, it was discovered that the network diagrams had not been updated to reflect the new changes. What is the MAJOR consequence of not having updated diagrams in such a scenario?

- (A) The servers might need a hardware upgrade
- (B) The company might need to revert to the old load balancer configuration
- (C) It increases the time and complexity of troubleshooting
- (D) Customers might prefer other logistics companies

Answers 1-110

Question 1. A client disputes having signed a digital contract. The service provider needs to prove that the signature was indeed from the client and hasn't been tampered with. Which of the following security concepts is the service provider relying on?

- (A) Authentication
- (B) Confidentiality
- (C) **Non-repudiation**
- (D) Access Control

Explanation 1. Correct Answer: C. Non-repudiation. Non-repudiation ensures that a party in a dispute cannot deny the authenticity of their actions. In this scenario, it would provide evidence that the client did sign the contract and that it hasn't been tampered with post-signature.

Option A is incorrect. Authentication confirms the identity of a user or system. While it plays a part in ensuring that the right person is accessing the system, it doesn't directly provide evidence about the actions post-authentication, like signing a contract.

Option B is incorrect. Confidentiality ensures that information is only accessible to those with the appropriate permissions. It doesn't provide evidence of an action being taken by a specific entity.

Option D is incorrect. Access Control determines who or what can view or use resources in a computing environment. It doesn't ensure the validity of actions taken within the system.

Question 2. Carlos, an IT consultant, advises a startup company on cybersecurity best practices. The company plans to launch several microsites under various subdomains. They want a solution that is cost-effective but also ensures that the sites are validated by a third-party. What type of certificate should Carlos recommend?

- (A) A separate self-signed certificate for each microsite
- (B) An individual third-party certificate for each subdomain
- (C) **A third-party wildcard certificate**
- (D) An EV certificate issued by an internal CA

Explanation 2. Correct Answer: C. A third-party wildcard certificate. A third-party wildcard certificate allows an organization to secure multiple subdomains with a single certificate. It's cost-effective as the company doesn't need to purchase and manage separate certificates for each subdomain, and because it's issued by a third-party Certificate Authority, it provides validation for external users.

Option A is incorrect. Self-signed certificates won't provide third-party validation, which could result in trust issues for external users.

Option B is incorrect. While individual third-party certificates for each subdomain will provide third-party validation, this approach would not be as cost-effective as a wildcard certificate.

Option D is incorrect. An EV certificate provides high assurance, but one issued by an internal CA will not be inherently trusted by external users.

Question 3. A company wants to ensure that security incidents are detected and addressed as quickly as possible by on-duty personnel. Which of the following operational security controls would be BEST to implement for this purpose?

- (A) Deploying a Network Intrusion Prevention System (NIPS)
- (B) Establishing a 24/7 Security Operations Center (SOC)
- (C) Creating a company-wide security policy
- (D) Implementing end-to-end data encryption

Explanation 3. Correct Answer: B. Establishing a 24/7 Security Operations Center (SOC). A Security Operations Center (SOC) is an operational control that provides real-time monitoring, detection, and response to security incidents. With a 24/7 SOC, the company ensures that there is always personnel available to handle security incidents as they occur.

Option A is incorrect. Deploying a Network Intrusion Prevention System (NIPS) is a technical control. While it can prevent unauthorized activities on the network, it does not ensure that there is personnel available around the clock to address incidents.

Option C is incorrect. Creating a company-wide security policy is a managerial control. It sets the guidelines and

procedures for security but does not ensure continuous monitoring and immediate response to incidents.

Option D is incorrect. Implementing end-to-end data encryption is a technical control that ensures data confidentiality. While it protects data, it does not ensure that incidents are detected and addressed by on-duty personnel in real-time.

Question 4. During a routine check, the IT department discovered that several employees had left their computers on and unattended during lunch break. Which operational security control can help mitigate the risk associated with this behavior?

- (A) Implementing biometric authentication
- (B) Enforcing a strict password policy
- (C) **Deploying an automatic screen lock after inactivity**
- (D) Implementing a secure coding practice

Explanation 4. Correct Answer: C. Deploying an automatic screen lock after inactivity. Deploying an automatic screen lock after a certain period of inactivity is an operational control. It ensures that unattended devices are protected from unauthorized access, thereby mitigating risks associated with employees leaving their computers on and unattended.

Option A is incorrect. Implementing biometric authentication is a technical control. While it enhances security at the point of access, it doesn't ensure that active sessions on unattended devices are secured against unauthorized access.

Option B is incorrect. Enforcing a strict password policy is a managerial control that dictates the creation and use of strong passwords. While it enhances access security, it doesn't secure active sessions on unattended devices.

Option D is incorrect. Implementing a secure coding practice is a technical and sometimes managerial control. It ensures software is written to prevent vulnerabilities but doesn't directly address the risk of unattended computers.

Question 5. An art gallery wants to deploy a security solution to detect movement in an open courtyard that features several sculptures. This space has varying temperature conditions, which might cause false alarms in some motion detection technologies. Which type of sensor would be MOST appropriate to ensure consistent motion detection in such conditions?

- (A) Thermal imaging sensors
- (B) Pressure-sensitive mats
- (C) Ultrasonic detectors
- (D) **Microwave motion detectors**

Explanation 5. Correct Answer: D. Microwave motion detectors. Microwave motion detectors are suitable for open areas and are less affected by temperature changes. They emit microwave beams to create an invisible detection zone and can consistently detect motion when an object interrupts this zone, irrespective of the ambient temperature.

Option A is incorrect. Thermal imaging sensors detect variations in heat. While they can be effective, the varying

temperature conditions in the courtyard may cause inconsistencies in detection.

Option B is incorrect. Pressure-sensitive mats are designed to detect weight or pressure changes when stepped on. They would not be suitable for an open courtyard where movement needs to be detected across a larger area.

Option C is incorrect. Ultrasonic detectors emit sound waves to detect motion. However, they might also be affected by external environmental factors and are not as suitable for open courtyards as microwave motion detectors.

Question 6. A company's primary security control for accessing secure server rooms is a biometric fingerprint scanner. However, the scanner occasionally malfunctions in high humidity. The security team is considering an alternative solution to grant access when the primary method fails. Which of the following would be the MOST appropriate compensating control?

- (A) **Implementing a security token-based authentication system**
- (B) Employing security guards at the main entrance
- (C) Installing security cameras inside the server room
- (D) Conducting regular server room audits

Explanation 6. Correct Answer: A. Implementing a security token-based authentication system. A security token-based authentication system would act as an alternative method for verifying the identity of individuals when the primary control

(biometric fingerprint scanner) fails. This serves as a direct compensating control for access.

Option B is incorrect. While security guards at the main entrance can provide an added layer of security, they aren't a direct compensating control for a malfunctioning biometric system in a specific location like the server room.

Option C is incorrect. While security cameras provide surveillance, they don't act as an alternative method for granting or denying access to the server room.

Option D is incorrect. Conducting regular server room audits is a detective control. It won't provide real-time access or compensate for the malfunctioning fingerprint scanner.

Question 7. A financial institution wants to ensure that customers are aware of the bank's policies on information sharing and how their personal data is used. Which of the following security controls would BEST communicate this to customers?

- (A) Implementing end-to-end encryption for online transactions
- (B) **Publishing a privacy policy on the bank's website**
- (C) Conducting annual cybersecurity awareness training for employees
- (D) Using multi-factor authentication for online banking

Explanation 7. Correct Answer: B. Publishing a privacy policy on the bank's website. A privacy policy serves as a directive control as it informs customers about the bank's

practices regarding the collection, use, and sharing of their personal data. By reading the policy, customers understand their rights and the bank's responsibilities.

Option A is incorrect. While end-to-end encryption ensures the confidentiality of online transactions, it doesn't inform customers about the bank's policies on information sharing or how their data is used.

Option C is incorrect. Annual cybersecurity awareness training is aimed at employees, not customers. It wouldn't directly communicate the bank's information-sharing policies to its customers.

Option D is incorrect. Using multi-factor authentication improves the security of online banking by requiring multiple forms of verification. However, it doesn't communicate to customers how their personal data is used or the bank's information-sharing policies.

Question 8. A large financial organization wants to ensure that all employees understand the importance of cybersecurity and the role they play in safeguarding company assets. Which of the following managerial security controls will be MOST effective in achieving this?

- (A) Installing a firewall at the network perimeter
- (B) **Regular security awareness training for employees**
- (C) Deploying an Intrusion Detection System (IDS)
- (D) Encrypting all company data

Explanation 8. Correct Answer: B. Regular security awareness training for employees. Security awareness training is a managerial control aiming to educate employees about security risks and the necessary precautions they need to take. By regularly training employees, the organization ensures that all staff are aware of potential threats and their roles in cybersecurity.

Option A is incorrect. Installing a firewall is a technical control focused on preventing unauthorized access to or from a private network. While it protects the network, it doesn't directly educate employees about their roles in cybersecurity.

Option C is incorrect. Deploying an Intrusion Detection System (IDS) is a technical control. It monitors network traffic for suspicious activities but does not directly focus on educating employees.

Option D is incorrect. Encrypting company data is a technical control. While it ensures the confidentiality of data, it doesn't address the employees' knowledge or awareness regarding cybersecurity.

Question 9. A company has faced multiple instances of unauthorized individuals gaining access to their office premises. Which of the following preventive security controls would be MOST effective in preventing unauthorized physical access?

(A) Implementing a log monitoring solution for network traffic

(B) Installing video surveillance cameras at all entry and exit points

- (C) Conducting regular security awareness training for employees
- (D) Implementing a multi-factor authentication system for network access.

Explanation 9. Correct Answer: B. Installing video surveillance cameras at all entry and exit points. Installing video surveillance cameras at all entry and exit points acts as a preventive control by deterring unauthorized individuals from attempting to gain access, given the increased risk of detection and recording.

Option A is incorrect. Implementing a log monitoring solution is a detective control that provides insights into network activities but doesn't prevent unauthorized physical access.

Option C is incorrect. Conducting regular security awareness training is a preventive measure, but its main focus is on making employees aware of security risks and best practices, not directly preventing unauthorized physical access.

Option D is incorrect. Implementing a multi-factor authentication system is a preventive control for unauthorized digital access but doesn't address the prevention of unauthorized physical access.

Question 10. TechVault, a company specializing in secure storage solutions, recently had an unauthorized intrusion where a burglar managed to bypass their motion sensors. In a bid to prevent future breaches, they are considering deploying a system that can detect weight changes in a restricted floor area

to alert any unauthorized access. Which of the following would be BEST for this requirement?

- (A) Ultrasonic motion detectors
- (B) **Pressure-sensitive floor mats**
- (C) CCTV cameras with facial recognition
- (D) Glass break sensors

Explanation 10. Correct Answer: B. Pressure-sensitive floor mats. Pressure-sensitive floor mats are designed to detect weight changes or pressure when stepped on. This makes them an effective solution for monitoring restricted areas and alerting unauthorized access based on weight detection.

Option A is incorrect. Ultrasonic motion detectors use sound waves to detect motion in an area but do not measure weight or pressure.

Option C is incorrect. CCTV cameras with facial recognition provide visual surveillance and can identify individuals, but they don't detect weight changes on the floor.

Option D is incorrect. Glass break sensors detect the sound of breaking glass and are primarily used for windows and glass doors, not for detecting pressure or weight changes on a floor.

Question 11. A system administrator is setting up an authentication system for a new web application. Which of the following security controls falls under the technical category and ensures that users prove their identity before gaining access?

- (A) Implementing a security awareness training program

- (B) Conducting a background check for new employees
- (C) **Using multi-factor authentication**
- (D) Establishing a clean desk policy

Explanation 11. Correct Answer: C. Using multi-factor authentication. Multi-factor authentication is a technical control that requires users to present two or more pieces of evidence (factors) before gaining access. It provides an additional layer of security to ensure that users are who they say they are.

Option A is incorrect. Implementing a security awareness training program is an administrative control, as it involves educating employees on security best practices rather than using technical measures to enforce them.

Option B is incorrect. Conducting a background check is an administrative control as it involves vetting potential employees before they're hired. This process doesn't directly enforce technical measures on systems or networks.

Option D is incorrect. Establishing a clean desk policy is an administrative control. It sets a guideline for employees to keep their workspaces tidy and free of sensitive information, rather than enforcing technical measures.

Question 12. An e-commerce company has experienced a Distributed Denial of Service (DDoS) attack, which caused its website to become inaccessible for several hours. To mitigate the impact of such attacks in the future, which of the following would be the BEST corrective control to implement?

- (A) Displaying a seal for third-party security certifications on the website
- (B) Establishing a Web Application Firewall (WAF) with DDoS protection**
- (C) Conducting routine vulnerability assessments on the website
- (D) Implementing strong password policies for website administrators

Explanation 12. Correct Answer: B. Establishing a Web Application Firewall (WAF) with DDoS protection. A Web Application Firewall (WAF) with DDoS protection can identify and filter out malicious traffic associated with DDoS attacks. As a corrective control, it can help in mitigating the impact and restoring normal service during and after an attack.

Option A is incorrect. Displaying a seal for third-party security certifications on the website acts as a deterrent by showing visitors and potential attackers that the site adheres to security standards. However, it does not mitigate or correct the effects of a DDoS attack.

Option C is incorrect. Conducting routine vulnerability assessments is a detective control that helps in identifying weaknesses. While it's essential for overall security, it doesn't directly correct or mitigate the effects of a DDoS attack.

Option D is incorrect. Implementing strong password policies for website administrators is a preventive control. It ensures that administrators' accounts are secure, but it does not address or correct the issues caused by a DDoS attack.

Question 13. GreenTech Industries has a manufacturing facility located in a relatively secluded area. Recent incidents of theft and trespassing have alarmed the management. Which of the following would MOST effectively deter unauthorized nighttime access to the perimeter of the facility?

- (A) Installing infrared sensors
- (B) **Using bright perimeter lighting**
- (C) Deploying additional security guards inside the facility
- (D) Increasing the height of the facility walls

Explanation 13. Correct Answer: B. Using bright perimeter lighting. Bright perimeter lighting acts as a strong deterrent for unauthorized individuals, as it reduces hiding spots, makes surveillance cameras more effective, and can make it easier for security personnel to spot potential threats. In secluded areas, proper lighting is particularly essential to illuminate dark spots and deter potential intruders.

Option A is incorrect. While infrared sensors can detect movement, they do not act as a visible deterrent in the same way bright lighting does.

Option C is incorrect. Deploying additional security guards inside the facility does not address the immediate concern of unauthorized nighttime access to the perimeter.

Option D is incorrect. Increasing the height of the walls can act as a deterrent, but it doesn't illuminate or expose potential intruders like bright lighting does.

Question 14. While conducting a routine security review, Jake, a security specialist, discovers an unexpected piece of data placed in the organization’s financial system. Upon asking, he learns that this piece of data is intentionally placed and monitored to see if any unauthorized user or system interacts with it. What is this deceptive piece of data known as?

- (A) Honeystring
- (B) **Honeytoken**
- (C) Canary token
- (D) Security marker

Explanation 14. Correct Answer: B. Honeytoken.

Honeytokens are strategically placed deceptive pieces of data that have no actual value or real-world use but are closely monitored. Their sole purpose is to detect unauthorized interactions, as any access or use of a honeytoken is likely malicious or unauthorized.

Option A is incorrect. There isn’t a commonly recognized security term known as “Honeystring” in the context described.

Option C is incorrect. Canary tokens are a specific type of honeytoken and can serve the same purpose. However, given the choices provided and the context of the question, “Honeytoken” is the most accurate answer.

Option D is incorrect. A security marker, in a general sense, can be any mark or indicator used for security purposes, but it isn’t specifically a deceptive piece of data placed to detect unauthorized access.

Question 15. An organization is deploying new IoT devices in its smart office. To ensure that only authorized devices can connect to the corporate network, each device will be given a unique key pair. Which of the following best describes the system authentication approach the organization is using?

- (A) Shared secret authentication
- (B) **Public key infrastructure (PKI)**
- (C) Token-based authentication
- (D) Username and password authentication

Explanation 15. Correct Answer: B. Public key infrastructure (PKI). Public key infrastructure (PKI) is a combination of hardware, software, policies, and standards that work together to provide a framework for secure communications. One of the primary features of PKI is the use of a pair of keys (public and private) to authenticate entities. In the scenario, each IoT device is given a unique key pair, indicating the use of PKI for system authentication.

Option A is incorrect. Shared secret authentication typically involves two parties having a shared secret that they use to authenticate one another. The scenario mentions a unique key pair for each device, which doesn't align with the concept of a shared secret.

Option C is incorrect. Token-based authentication typically involves using a hardware or software token that generates a time-sensitive code. The scenario is describing the use of key pairs, not tokens.

Option D is incorrect. Username and password authentication is a method where entities provide a username and a secret password to verify their identity. The scenario does not mention the use of usernames or passwords.

Question 16. In the new branch of BankSecure, the management has decided to install a security system at the main entrance that forces visitors to go through two separate authorization checks before entering the main premises. Which physical security measure should they consider?

- (A) Turnstiles
- (B) Security Guards
- (C) **Access Control Vestibule**
- (D) Keycard Readers

Explanation 16. Correct Answer: C. Access Control

Vestibule. An access control vestibule, often referred to as a mantrap, is a two-stage authentication system. It consists of two doors: a person enters the first door, undergoes an authorization check (like a badge reader or biometric scanner), and only after being approved can they proceed to the second door, where they undergo another authorization check before accessing the main premises.

Option A is incorrect. Turnstiles control the flow of individuals into a location and can prevent tailgating to some extent, but they do not force a two-stage authorization check.

Option B is incorrect. While security guards can perform authorization checks and control access, they alone do not

provide a two-stage authorization system like an access control vestibule.

Option D is incorrect. Keycard readers are a form of access control that checks the credentials of individuals, but on their own, they don't ensure two separate authorization checks.

Question 17. The IT department wants to monitor network traffic in real time to detect any anomalies or malicious activities. Which of the following security controls can accomplish this?

- (A) Security policy documentation
- (B) **Intrusion Detection System (IDS)**
- (C) Employee code of conduct
- (D) Access Control Lists (ACL)

Explanation 17. Correct Answer: B. Intrusion Detection System (IDS). An Intrusion Detection System (IDS) is a technical control that monitors network traffic in real-time and alerts administrators to any suspicious or malicious activities based on predefined rules or heuristics.

Option A is incorrect. Security policy documentation is an administrative control. It provides guidelines and procedures for maintaining security but does not actively monitor network traffic.

Option C is incorrect. Employee code of conduct is an administrative control. It provides guidelines on how employees should behave in a professional setting but does not actively monitor network traffic.

Option D is incorrect. Access Control Lists (ACL) are technical controls, but they are used to define permissions on who can access specific resources. They do not actively monitor network traffic in real-time for anomalies or malicious activities.

Question 18. Jenna, a web administrator for a growing online retail business, is in the process of obtaining SSL certificates for the company's domain. The company uses several subdomains for different services, such as shop.example.com, blog.example.com, and support.example.com. Instead of obtaining individual certificates for each subdomain, Jenna wants to use one certificate. What type of certificate should Jenna pursue?

- (A) Extended Validation Certificate
- (B) **Wildcard Certificate**
- (C) Certificate with Subject Alternative Names (SAN)
- (D) Code Signing Certificate

Explanation 18. Correct Answer: B. Wildcard Certificate. A Wildcard Certificate is designed to secure a domain and its subdomains under the same top-level domain. For example, a wildcard certificate for *.example.com would secure shop.example.com, blog.example.com, and any other subdomain of example.com.

Option A is incorrect. An Extended Validation Certificate provides the highest level of validation but does not necessarily cover multiple subdomains by default.

Option C is incorrect. While a Certificate with Subject Alternative Names (SAN) can secure multiple domains and subdomains, it is not specifically tailored for all subdomains under a single domain as the Wildcard Certificate is.

Option D is incorrect. A Code Signing Certificate is used to sign software code, ensuring its integrity and authenticity, not for securing domains or subdomains.

Question 19. At a newly established museum, management wants to install sensors in the exhibit rooms to detect any unauthorized movement after hours. The rooms are often filled with a mix of air conditioning and external noise from the city. Which sensor would be BEST suited to detect movement in such conditions without being affected by the noise?

- (A) Acoustic sensors
- (B) Glass break detectors
- (C) **Ultrasonic sensors**
- (D) Thermal imaging cameras

Explanation 19. Correct Answer: C. Ultrasonic sensors.

Ultrasonic sensors emit high-frequency sound waves to detect motion. These sound waves are beyond the range of human hearing and won't be affected by ambient noise, making them ideal for environments with varying noise conditions. When motion is detected, as indicated by changes in the reflected waves, an alarm is triggered.

Option A is incorrect. Acoustic sensors detect specific sounds. The external noise from the city might cause false alarms or interfere with their detection capabilities.

Option B is incorrect. Glass break detectors are designed to detect the sound or vibration of breaking glass. They aren't designed primarily to detect movement.

Option D is incorrect. Thermal imaging cameras detect heat signatures and would be more susceptible to variations in room temperature due to air conditioning, potentially leading to false detections.

Question 20. A company is setting up a secure communication channel between its headquarters and a remote branch office. To ensure that data transmitted over this channel originates from a legitimate system at the branch office, the company is considering using digital certificates. Which authentication method for systems is the company contemplating?

- (A) Kerberos authentication
- (B) Password-based authentication
- (C) **Certificate-based authentication**
- (D) Biometric-based authentication

Explanation 20. Correct Answer: C. Certificate-based authentication. Certificate-based authentication uses digital certificates to verify the identity of systems or individuals. In the given scenario, the company wants to verify that data transmitted over the communication channel originates from a legitimate system, making digital certificates an appropriate choice.

Option A is incorrect. Kerberos authentication is a ticket-based authentication protocol primarily used to authenticate users in a

network, not specifically for system-to-system authentication using digital certificates.

Option B is incorrect. Password-based authentication requires systems or users to provide a secret password to prove their identity. It doesn't involve the use of digital certificates.

Option D is incorrect. Biometric-based authentication involves using unique physical or behavioral attributes of a person for verification, such as fingerprints or facial patterns. It is not applicable to system-to-system authentication.

Question 21. A financial institution has experienced an uptick in unauthorized transactions. They want to implement a control that will allow them to identify suspicious transactions in real-time. Which of the following would be the BEST detective control for this scenario?

- (A) Implementing a multi-factor authentication system for all users
- (B) Establishing a Security Operations Center (SOC) to monitor network traffic
- (C) **Installing an Intrusion Detection System (IDS) on their network**
- (D) Restricting transaction capabilities to only a few trusted IP addresses.

Explanation 21. Correct Answer: C. Installing an Intrusion Detection System (IDS) on their network. An Intrusion Detection System (IDS) serves as a detective control by monitoring network traffic for suspicious activities and potential threats. In this context, it can be configured to detect patterns

related to unauthorized transactions, thereby allowing timely intervention.

Option A is incorrect. Implementing a multi-factor authentication system is a preventive control that provides an additional layer of security by requiring two or more verification methods. While it reduces the risk of unauthorized access, it does not detect suspicious transactions.

Option B is incorrect. Establishing a Security Operations Center (SOC) is a broad approach to handle security events, and while it can include detective controls, merely setting up a SOC does not provide specific real-time detection of unauthorized transactions.

Option D is incorrect. Restricting transaction capabilities to only a few trusted IP addresses is a preventive control that limits the sources of potential transactions. While it can reduce the number of unauthorized transactions, it does not detect them.

Question 22. TechHaus has recently experienced multiple security breaches where unauthorized personnel have managed to infiltrate their server rooms after hours. To enhance security measures, the company decided to deploy a new system. Which of the following options would BEST detect human intruders based on their body heat even in complete darkness?

- (A) Installing CCTV cameras with LED lights
- (B) Using ultrasonic motion sensors
- (C) **Deploying infrared (IR) sensors**
- (D) Implementing RFID badge readers at the entrance

Explanation 22. Correct Answer: C. Deploying infrared (IR) sensors. Infrared (IR) sensors detect infrared radiation, such as the heat emitted by the human body. This makes them particularly effective in detecting human intruders, even in complete darkness, based on the body heat they emit.

Option A is incorrect. While CCTV cameras with LED lights can provide visual surveillance, they rely on light to produce images and may not detect intruders in complete darkness as efficiently as infrared sensors.

Option B is incorrect. Ultrasonic motion sensors detect movement through sound waves, not body heat, making them less efficient in differentiating between a human intruder and other moving objects.

Option D is incorrect. RFID badge readers control access at entry points but do not detect human intruders based on their body heat inside a facility.

Question 23. After detecting an unauthorized intrusion into their network, a financial institution wants to implement a control that will restore compromised systems to a known good state. Which of the following would be the MOST appropriate corrective control?

- (A) Implementing Intrusion Detection Systems (IDS) across the network
- (B) Frequently updating firewall rules
- (C) **Restoring systems from verified backups**
- (D) Enabling multi-factor authentication for users

Explanation 23. Correct Answer: C. Deploying infrared (IR) sensors. Infrared (IR) sensors detect infrared radiation, such as the heat emitted by the human body. This makes them particularly effective in detecting human intruders, even in complete darkness, based on the body heat they emit.

Option A is incorrect. While CCTV cameras with LED lights can provide visual surveillance, they rely on light to produce images and may not detect intruders in complete darkness as efficiently as infrared sensors.

Option B is incorrect. Ultrasonic motion sensors detect movement through sound waves, not body heat, making them less efficient in differentiating between a human intruder and other moving objects.

Option D is incorrect. RFID badge readers control access at entry points but do not detect human intruders based on their body heat inside a facility.

Question 24. After a recent security breach, Sarah, a cybersecurity analyst, is implementing additional measures to detect unauthorized activities. She decides to embed specific values in the database that serve no real purpose but are monitored for any unauthorized access or usage. These values are designed to raise alerts if they are ever accessed or used. What are these specific values commonly referred to as?

- (A) Security flags
- (B) Honeypots
- (C) **Honeytokens**
- (D) Audit trails

Explanation 24. Correct Answer: C. Restoring systems from verified backups. Restoring systems from verified backups is a corrective control, as it can restore compromised systems to their last known good state. This action corrects the adverse effects of the intrusion and ensures that any malicious alterations are removed.

Option A is incorrect. Implementing Intrusion Detection Systems (IDS) is a detective control. It monitors and detects malicious activities in the network but doesn't correct the adverse impacts of an intrusion.

Option B is incorrect. Frequently updating firewall rules is a preventive measure, aiming to block malicious traffic and prevent potential intrusions. While vital, it doesn't correct the impacts of an already occurred breach.

Option D is incorrect. Enabling multi-factor authentication is a preventive control, aiming to provide additional layers of verification. While it enhances security, it doesn't correct the adverse impacts of an intrusion.

Question 25. Bob receives an email prompting him to verify his identity by clicking on a link. The link directs him to a webpage where he has to provide his username, password, and answer a personal security question. What type of authentication method is being employed here?

- (A) Biometric authentication
- (B) Token-based authentication
- (C) **Two-factor authentication**
- (D) Single sign-on

Explanation 25. Correct Answer: C. Two-factor

authentication. Two-factor authentication (2FA) is a security process in which users provide two different authentication factors to verify their identity. In this scenario, Bob is providing something he knows (username and password) and also answering a personal security question, which is another form of “something he knows.”

Option A is incorrect. Biometric authentication involves using unique physical or behavioral attributes of a person for verification, such as fingerprints or facial patterns. The scenario doesn’t mention any biometric data.

Option B is incorrect. Token-based authentication typically involves using a hardware or software token that generates a time-sensitive code. This was not described in the scenario.

Option D is incorrect. Single sign-on (SSO) allows a user to log in once and gain access to multiple systems without being prompted to log in again for each system. The scenario describes a two-factor authentication process, not SSO.

Question 26. In an effort to minimize data breaches from malware, a company is deciding on a control to prevent malicious software from being executed on company devices. Which of the following would be the BEST preventive control?

- (A) Deploying a Network Intrusion Detection System (NIDS)
- (B) Regularly backing up critical data
- (C) **Installing an antivirus software with real-time**

scanning

(D) Performing a forensic analysis after a security incident

Explanation 26. Correct Answer: C. Two-factor

authentication. Two-factor authentication (2FA) is a security process in which users provide two different authentication factors to verify their identity. In this scenario, Bob is providing something he knows (username and password) and also answering a personal security question, which is another form of “something he knows.”

Option A is incorrect. Biometric authentication involves using unique physical or behavioral attributes of a person for verification, such as fingerprints or facial patterns. The scenario doesn't mention any biometric data.

Option B is incorrect. Token-based authentication typically involves using a hardware or software token that generates a time-sensitive code. This was not described in the scenario.

Option D is incorrect. Single sign-on (SSO) allows a user to log in once and gain access to multiple systems without being prompted to log in again for each system. The scenario describes a two-factor authentication process, not SSO.

Question 27. After undergoing a major infrastructure upgrade, GlobalMed Corp experienced several unanticipated security issues. In retrospect, the IT manager realized they skipped an essential step in their change management process which could have predicted and mitigated these issues. What step did they most likely overlook?

- (A) Procurement of new hardware
- (B) Training of IT staff on the new systems
- (C) **Impact analysis**
- (D) Integration with legacy systems

Explanation 27. Correct Answer: C. Impact analysis. An impact analysis is vital in the change management process as it evaluates the potential ramifications of a proposed change. By conducting this analysis, organizations can anticipate potential security challenges and mitigate them before implementing the change.

Option A is incorrect. While procurement is essential, merely purchasing new hardware wouldn't directly help in predicting or mitigating potential security issues stemming from an infrastructure upgrade.

Option B is incorrect. Training IT staff is essential for effective implementation and operation, but it doesn't directly address predicting and understanding potential security consequences of the upgrade.

Option D is incorrect. Integration with legacy systems is a crucial consideration, especially for compatibility. However, the focus of the scenario is on predicting and understanding potential security issues, which is primarily addressed through an impact analysis.

Question 28. MegaCorp recently introduced a new web application for its customers. Before its release, the software underwent rigorous testing in a controlled environment. When

the application was deployed in production, several security vulnerabilities were reported. Which of the following reasons can explain the mismatch between the test results and actual vulnerabilities?

- (A) The testing environment was an exact replica of the production environment
- (B) **Test results were not thoroughly reviewed**
- (C) The software was not tested for zero-day vulnerabilities
- (D) Penetration testing was done post-production

Explanation 28. Correct Answer: B. Test results were not thoroughly reviewed. Even if an application is tested rigorously, it is crucial to thoroughly review and interpret the test results to identify any potential security vulnerabilities. Failing to review or misinterpreting these results can lead to vulnerabilities going unnoticed and unresolved.

Option A is incorrect. Having a testing environment that mirrors the production environment is a best practice. This ensures that the tests are representative of how the software will behave in production.

Option C is incorrect. While zero-day vulnerabilities are a concern, by definition, they are unknown vulnerabilities. Testing specifically for them would be challenging. However, thorough testing and review processes can mitigate potential risks.

Option D is incorrect. Penetration testing is an essential aspect of security testing, but doing it post-production doesn't explain

the mismatch between the test results and actual vulnerabilities if the initial test results were not reviewed correctly.

Question 29. An online banking website employs a system that automatically logs out users after 10 minutes of inactivity to ensure that if a user forgets to log out, no one else can alter the user's banking details. Which principle of the CIA triad is the banking website MOST directly addressing?

- (A) Confidentiality
- (B) Availability
- (C) Authentication
- (D) **Integrity**

Explanation 29. Correct Answer: D. Integrity. The integrity pillar of the CIA triad ensures the accuracy and reliability of data. By logging out users after a period of inactivity, the banking website aims to prevent unauthorized modifications (potentially by someone else who might gain access to the unattended session) to the user's banking details, thereby maintaining the integrity of the data.

Option A is incorrect. While logging out users does have a confidentiality aspect, the primary aim in this scenario is to prevent unauthorized changes rather than unauthorized viewing.

Option B is incorrect. Availability ensures that data and systems are accessible to authorized users when they need it. This scenario doesn't discuss providing or restricting access based on system uptime or accessibility.

Option C is incorrect. Authentication ensures that users are who they claim to be. While the scenario does touch on security measures, the primary concern here is preventing unauthorized changes to data, which aligns with integrity, not authentication.

Question 30. A company is located in an area prone to natural disasters such as earthquakes and floods. Which of the following physical security controls would be MOST effective in ensuring the safety of the company's IT infrastructure?

- (A) Using biometric authentication for server access
- (B) Deploying a firewall to protect against cyber threats
- (C) **Establishing a raised floor system in the data center**
- (D) Conducting penetration testing on a regular basis

Explanation 30. Correct Answer: C. Establishing a raised floor system in the data center. A raised floor system in a data center serves as a physical control by elevating equipment off the ground, helping to protect it from potential water damage in the event of flooding and providing some protection from other environmental risks.

Option A is incorrect. Using biometric authentication is a technical control that enhances security by confirming users' identities based on physical or behavioral attributes. While it strengthens access security, it doesn't provide protection against natural disasters.

Option B is incorrect. Deploying a firewall is a technical control that guards against unauthorized access to or from a private network. While it protects against cyber threats, it

doesn't offer protection against physical threats like natural disasters.

Option D is incorrect. Conducting penetration testing is a technical and sometimes operational control that identifies vulnerabilities in an organization's digital assets. While it enhances cyber security, it doesn't protect infrastructure against physical threats.

Question 31. TechBank has just opened a new branch in the city center. Due to its location, the management is concerned about potential vehicular attacks on the facility. Which of the following physical security measures can TechBank employ to specifically deter such attacks?

- (A) Surveillance Cameras
- (B) **Bollards**
- (C) Access Badges
- (D) Security Guards

Explanation 31. Correct Answer: B. Bollards. Bollards are short, sturdy vertical posts that are typically used to control road traffic. In the context of physical security, they serve to prevent vehicles from entering areas where they are not allowed, thereby acting as a deterrent against potential vehicular attacks.

Option A is incorrect. While surveillance cameras can monitor and record activities, they do not serve as a physical barrier against vehicular attacks.

Option C is incorrect. Access badges control personnel access to facilities but do not deter vehicular attacks.

Option D is incorrect. While security guards can respond to threats and control access, they are not a specific measure to deter vehicular attacks like bollards.

Question 32. During a security assessment, Maria, a security consultant, identifies a self-signed certificate being used on a client's public-facing web server. What is the PRIMARY security concern related to this finding?

- (A) The web server might be vulnerable to Distributed Denial of Service (DDoS) attacks
- (B) The certificate could be expired
- (C) **Users cannot validate the authenticity of the website easily**
- (D) The web server might not support modern encryption algorithms

Explanation 32. Correct Answer: C. Users cannot validate the authenticity of the website easily. Self-signed certificates are not signed by a recognized Certificate Authority. As a result, when users connect to a website using a self-signed certificate, they typically receive a warning that the certificate is not trusted. This poses a risk as users cannot easily validate the authenticity of the website, making them more susceptible to man-in-the-middle attacks.

Option A is incorrect. While DDoS attacks are a concern for public-facing web servers, they aren't directly related to the use of self-signed certificates.

Option B is incorrect. Any certificate, whether self-signed or CA-signed, can expire. However, expiration is not the primary

concern related to the use of self-signed certificates on public-facing servers.

Option D is incorrect. The use of modern encryption algorithms is independent of whether a certificate is self-signed or not.

Question 33. TechFin Bank is considering implementing a new software system for their transaction processing. Before rolling it out, the cybersecurity team insists on carrying out a specific type of analysis to understand how this change might affect the organization's security posture. What is the team referring to?

- (A) Risk appetite assessment
- (B) Performance benchmarking
- (C) **Impact analysis**
- (D) Penetration testing

Explanation 33. Correct Answer: C. Impact analysis. An impact analysis assesses the potential consequences of a change within an organization. In the context of TechFin Bank, the cybersecurity team would use this analysis to understand how the new software system might introduce new vulnerabilities, affect existing security measures, or otherwise impact the bank's overall security.

Option A is incorrect. Risk appetite assessment refers to determining the amount and type of risk an organization is willing to accept in pursuit of its objectives. It doesn't focus on the consequences of a specific change.

Option B is incorrect. Performance benchmarking focuses on comparing an organization's performance metrics to industry standards or best practices, not assessing the potential security impact of a change.

Option D is incorrect. While penetration testing is crucial to assess the vulnerabilities in a system, it doesn't provide a holistic view of the potential impacts a change might have on an organization's security posture.

Question 34. To discourage potential cybercriminals from targeting their online storefront, an e-commerce company is considering various security measures. Which of the following would act MOST effectively as a deterrent control?

- (A) **Displaying a seal for third-party security certifications on the website**
- (B) Using a Web Application Firewall (WAF)
- (C) Conducting monthly vulnerability assessments
- (D) Storing customer data in encrypted databases

Explanation 34. Correct Answer: A. Displaying a seal for third-party security certifications on the website. Displaying a seal for third-party security certifications on the website serves as a deterrent control. It sends a message to potential attackers that the site is recognized for its security measures, which can discourage them from attempting an attack.

Option B is incorrect. Using a Web Application Firewall (WAF) is a preventive control. It filters, monitors, and blocks malicious web traffic. While it helps in defending against cyber threats, it doesn't act as a visible deterrent to attackers.

Option C is incorrect. Conducting monthly vulnerability assessments is a detective control. It identifies vulnerabilities to enhance the security posture but doesn't act as a deterrent to potential attackers.

Option D is incorrect. Storing customer data in encrypted databases is a preventive control that ensures unauthorized individuals cannot access or comprehend the stored data. It protects data but doesn't deter potential cybercriminals.

Question 35. The security team of a multinational company deployed a network of honeypots globally, making it appear as an interconnected and realistic environment. They aim to study coordinated multi-stage attacks. This deceptive setup is known as:

- (A) Firewall Cluster
- (B) Virtual LAN (VLAN)
- (C) Distributed Denial of Service (DDoS) Prevention
- (D) **Honeynet**

Explanation 35. Correct Answer: D. Honeynet. A honeynet is essentially a network of honeypots. It is designed to be attractive to attackers, making them believe they are attacking a real network, while in reality, they are being observed, and their tactics and techniques are being analyzed.

Option A is incorrect. A Firewall Cluster is a group of firewalls operating together to increase reliability and performance. It doesn't serve as a decoy to attract attackers.

Option B is incorrect. A Virtual LAN (VLAN) is a network protocol used to create logically segmented networks within a physical network, improving performance and security. It's not a decoy system.

Option C is incorrect. Distributed Denial of Service (DDoS) Prevention solutions focus on identifying and mitigating large-scale attempts to disrupt network service availability. They do not present a deceptive environment for attackers.

Question 36. ExamsDigest Corp, a technology company, recently conducted a security assessment to align with industry best practices. The company's current security posture was compared to its desired future state, revealing discrepancies. Which of the following best describes the approach ExamsDigest Corp employed?

- (A) Vulnerability Assessment
- (B) Penetration Testing
- (C) **Gap Analysis**
- (D) Threat Modeling

Explanation 36. Correct Answer: C. Gap Analysis. Gap analysis is a method of comparing the current state of something (such as security measures) with a future desired state to identify the discrepancies or "gaps". In the scenario, ExamsDigest Corp compared their current security posture to a desired future state, which is consistent with the process of gap analysis.

Option A is incorrect. A vulnerability assessment focuses on identifying, quantifying, and ranking vulnerabilities in a system, not comparing the current state with a desired future state.

Option B is incorrect. Penetration testing is an authorized simulated cyberattack on a system to evaluate its security, not to compare its current state with a desired future state.

Option D is incorrect. Threat modeling is the process of identifying potential threats to a system and determining the risk they pose, not comparing the current state with a desired future state.

Question 37. A pharmaceutical company is concerned about competitors accessing their formula for a new drug. Which pillar of the CIA triad is MOST directly addressed by their concern?

- (A) Availability
- (B) **Confidentiality**
- (C) Integrity
- (D) Non-repudiation

Explanation 37. Correct Answer: B. Confidentiality. The confidentiality pillar of the CIA triad ensures that information is accessible only to those with authorized access. In this scenario, the company wants to ensure that its drug formula remains secret and is not accessible to unauthorized individuals, particularly competitors.

Option A is incorrect. Availability ensures that information is accessible to authorized users when needed. The concern here is

not about access to the data but rather about preventing unauthorized access.

Option C is incorrect. Integrity ensures the accuracy and reliability of data and systems. The scenario doesn't mention concerns about the formula being altered, only about unauthorized access.

Option D is incorrect. Non-repudiation is a concept ensuring that a party in a dispute cannot deny the authenticity of their actions. It's not directly related to the company's concern about the secrecy of their drug formula.

Question 38. FinCorp, a financial institution, has recently adopted a new security framework. In this framework, every device and user inside the organization's network is treated as if they were outside the perimeter, necessitating rigorous verification processes even for internal requests. Which security paradigm has FinCorp implemented?

- (A) Demilitarized Zone (DMZ)
- (B) Network Segmentation
- (C) Intrusion Detection System (IDS)
- (D) **Zero Trust**

Explanation 38. Correct Answer: D. Zero Trust. Zero Trust is a security model that treats every access request with skepticism, regardless of its origin, be it from within or outside the organization's traditional perimeter. It requires rigorous verification processes for every interaction.

Option A is incorrect. A Demilitarized Zone (DMZ) is a physical or logical subnetwork that exposes an organization's external-facing services to a larger, untrusted network, usually the internet.

Option B is incorrect. Network Segmentation divides a network into multiple segments or subnets, allowing administrators to control the flow of traffic between them. It does not inherently distrust all traffic like Zero Trust.

Option C is incorrect. Intrusion Detection System (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. It doesn't define how trust is managed across interactions.

Question 39. GreenValley Mall, located in a busy urban area, has recently faced security concerns due to the proximity of its main entrance to a major road. Which physical security enhancement can the mall management implement to create a protective barrier between the road and the entrance, ensuring pedestrian safety and preventing unauthorized vehicular access?

- (A) Reinforced Walls
- (B) Metal Detectors
- (C) **Bollards**
- (D) Perimeter Fencing

Explanation 39. Correct Answer: C. Bollards. Bollards are robust vertical posts, usually made of steel or concrete, which can be placed at specific intervals to form a protective barrier. They can effectively prevent vehicles from accessing pedestrian

areas or building entrances while allowing pedestrian movement.

Option A is incorrect. While reinforced walls can offer protection against various threats, they would not be practical for separating a mall entrance from a road as they would block pedestrian access as well.

Option B is incorrect. Metal detectors are used for detecting metal objects and weapons on individuals entering a facility, not for stopping vehicular access.

Option D is incorrect. Perimeter fencing can deter unauthorized access, but it might not specifically prevent fast-moving vehicular threats like bollards do. Furthermore, a fence might not be aesthetically pleasing or practical in front of a mall entrance.

Question 40. A tech company, InnovateTech, has recently faced multiple incidents of unauthorized personnel trying to access their R&D labs. They wish to monitor and record all activities near the entrance of this sensitive area. Which physical security measure would be most effective for this requirement?

- (A) RFID Badge Readers
- (B) Biometric Scanners
- (C) **Video Surveillance Cameras**
- (D) Mantrap

Explanation 40. Correct Answer: C. Video Surveillance Cameras. Video surveillance cameras provide a continuous visual monitoring capability and can record activities near

specific areas. For the purpose of observing and recording incidents near the entrance of the R&D labs, video surveillance would be the most direct and effective solution.

Option A is incorrect. While RFID badge readers can control access and log which badges are used at entrances, they do not visually monitor or record activities.

Option B is incorrect. Biometric scanners are an authentication mechanism, and while they offer a high level of security for access control, they do not provide visual monitoring or recording capabilities.

Option D is incorrect. A mantrap is a physical security access control system that prevents tailgating into secure areas. While it can enhance security at entrances, it does not visually record activities.

Question 41. A cybersecurity analyst at XYZ Corp is looking to deploy a system that appears to be vulnerable and enticing to attackers. The main goal is to study the tactics, techniques, and procedures (TTPs) of potential adversaries, without them realizing that they're interacting with a decoy. Which of the following would BEST meet this requirement?

- (A) Intrusion Detection System (IDS)
- (B) Firewall
- (C) **Honeypot**
- (D) VPN Concentrator

Explanation 41. Correct Answer: C. Honeypot. A honeypot is a security mechanism designed to lure attackers into interacting

with a seemingly vulnerable system. Its primary purpose is not to block or prevent attacks but to log and study them. By analyzing the activities on the honeypot, security professionals can gain insights into the methods and motivations of the attackers.

Option A is incorrect. An Intrusion Detection System (IDS) is designed to detect malicious activities on a network and alert administrators. While it can identify threats, it doesn't actively lure attackers.

Option B is incorrect. A firewall is designed to block or allow traffic based on specific rules. It doesn't present itself as a vulnerable target to lure attackers.

Option D is incorrect. A VPN Concentrator is a device that provides remote access to a network over a secure connection. Its primary purpose is to enable secure remote access, not to act as a decoy for attackers.

Question 42. A multinational organization recently experienced a significant security breach. After investigating, it was determined that a change to the network infrastructure was made without undergoing the standard approval process. As a result, there was a misconfiguration which allowed unauthorized access. What security principle related to change management did the organization neglect?

- (A) Configuration baseline reviews
- (B) **Least privilege enforcement**
- (C) Approval process adherence
- (D) Patch management

Explanation 42. Correct Answer: C. Approval process

adherence. The approval process is a critical aspect of change management. Before any changes are made, especially to critical systems like network infrastructure, they need to undergo a rigorous approval process. This ensures that multiple experts evaluate the change for potential vulnerabilities or issues. In this scenario, skipping the approval process led to a significant security breach.

Option A is incorrect. Configuration baseline reviews involve regularly checking and ensuring that systems are configured as per the organization's approved baseline. While it's important, the issue in the scenario was directly related to bypassing the approval process.

Option B is incorrect. Least privilege enforcement means providing only the minimal necessary access to users to perform their tasks. This scenario doesn't deal with access rights or privileges.

Option D is incorrect. Patch management concerns the process of applying updates to software and systems. The breach in the question wasn't related to missing patches but was due to bypassing the approval process.

Question 43. After a series of cyber-attacks on a company's infrastructure, the IT team decided to deploy a solution that would seem like a legitimate part of their network but is intentionally isolated and monitored. They intend to detect and analyze malicious activities in this isolated environment. What technology are they most likely implementing?

- (A) Network segmentation
- (B) **Honeypot**
- (C) DMZ (Demilitarized Zone)
- (D) Sandboxing

Explanation 43. Correct Answer: B. Honeypot. A honeypot is intentionally set up to appear as a legitimate part of a network, but it is isolated and closely monitored. Its purpose is to attract attackers and observe their actions, thereby providing insights into potential threats and the methods employed by adversaries.

Option A is incorrect. Network segmentation involves dividing a network into smaller sub-networks. While this can enhance security by limiting attackers' access to specific segments, it doesn't act as a decoy to attract attackers.

Option C is incorrect. A DMZ (Demilitarized Zone) is a subnet that acts as a buffer between the internet and an organization's internal network. While it can contain servers accessible to external users, its primary purpose is not to act as a decoy but to provide a layer of protection.

Option D is incorrect. Sandboxing is a security mechanism that allows programs to run in a separate environment to prevent them from affecting the broader system. It's used for testing and analyzing potentially malicious software, not for luring attackers.

Question 44. Liam, the CTO of a medium-sized enterprise, noticed that several software applications were not updated regularly, leading to potential security vulnerabilities. Upon

investigation, he realized that no specific team or individual was assigned as the owner of these applications. To enhance security, what should Liam emphasize?

- (A) Immediate decommissioning of all unowned applications
- (B) Assignment of clear ownership to all business applications**
- (C) Conducting monthly vulnerability assessments on all applications
- (D) Outsourcing the management of these applications to third-party vendors

Explanation 44. Correct Answer: B. Assignment of clear ownership to all business applications. Assigning clear ownership ensures that there's a designated team or individual responsible for the upkeep, updates, and security of an application. When there's clear ownership, the owner has the accountability to maintain and secure the application, reducing the risk of oversights like missing updates.

Option A is incorrect. Immediate decommissioning may not be practical or feasible, especially if the applications are critical to business operations.

Option C is incorrect. While monthly vulnerability assessments can help identify security issues, they don't address the root cause of the problem highlighted in the scenario – the lack of ownership and accountability.

Option D is incorrect. Outsourcing may shift the responsibility, but it doesn't ensure that the applications will be better managed

or more secure. Ownership clarity is paramount, whether the management is internal or outsourced.

Question 45. TechSoft Corp, a mid-sized software development firm, is relocating its main office to a new building. The management is concerned about potential threats after hours, particularly due to the increasing reports of cyber-espionage. They are evaluating different security measures. Which option would provide an immediate physical presence and deterrence during non-business hours?

- (A) CCTV with motion detection
- (B) Retinal scan at all entrances
- (C) **Security guard presence**
- (D) Reinforced doors and windows

Explanation 45. Correct Answer: C. Security guard presence. A security guard provides a visible deterrent and immediate physical presence. This human element is invaluable in situations where an immediate response to threats, deterrence of potential intruders, or evaluation of suspicious activities is required, especially during non-business hours.

Option A is incorrect. While CCTV with motion detection can monitor and alert on movement, it doesn't provide the immediate human response and deterrence a security guard does.

Option B is incorrect. A retinal scan is an authentication mechanism for controlling access. While it offers high security, it doesn't offer the visible deterrence or immediate response of a security guard.

Option D is incorrect. Reinforced doors and windows enhance the physical security of a building, but they don't provide an active and visible human deterrence like a security guard.

Question 46. Alice, a system administrator for a startup, is preparing to deploy a new website for her company. To ensure secure communications between the users and the website, she plans to obtain a digital certificate for the site. Before doing so, which step must Alice first undertake to get a certificate from a Certificate Authority (CA)?

- (A) **Generate a public-private key pair**
- (B) Submit her passport copy to the CA
- (C) Download the latest CA root certificate
- (D) Encrypt the website with symmetric encryption

Explanation 46. Correct Answer: A. Generate a public-private key pair. Before Alice can request a digital certificate from a CA, she must first generate a public-private key pair. Once this is done, she creates a Certificate Signing Request (CSR) containing her public key and some additional information. The CSR is then submitted to the CA for signing.

Option B is incorrect. CAs do not typically require a passport copy for standard SSL/TLS certificates. They might have identity verification processes, but it's usually for extended validation certificates.

Option C is incorrect. While it may be necessary to trust a CA by downloading its root certificate, this is not the step required before requesting a digital certificate.

Option D is incorrect. Symmetric encryption is unrelated to the process of obtaining a digital certificate.

Question 47. Julia, a security administrator, is concerned about potential unauthorized access to confidential project files stored on a company server. She decides to place a document within the project folders that seems enticing but is actually monitored for access. This strategy aims to detect if someone is accessing files without authorization. What is this document commonly known as?

- (A) Salt file
- (B) **Honeyfile**
- (C) Log file
- (D) Backup file

Explanation 47. Correct Answer: B. Honeyfile. A honeyfile is a monitored file placed intentionally to act as a decoy. If accessed, it can provide an alert that someone might be accessing files without proper authorization, or it might be an indication of a potential insider threat.

Option A is incorrect. A salt is random data that is used as an additional input to a one-way function that hashes data or passwords. It isn't a decoy file.

Option C is incorrect. A log file records events in an operating system or other software to aid in troubleshooting and activity monitoring, but it isn't used as a deceptive measure.

Option D is incorrect. A backup file is a copy of a file or database that can be used for data recovery. It's not a decoy to detect unauthorized access.

Question 48. After a recent incident of vandalism, a corporate building is considering implementing security controls that would dissuade potential perpetrators. Which of the following would serve BEST as a deterrent control?

- (A) Encrypting all stored data
- (B) Installing biometric access controls on all entrances
- (C) Implementing regular data backups
- (D) **Placing visible security signage indicating 24/7 surveillance**

Explanation 48. Correct Answer: D. Placing visible security signage indicating 24/7 surveillance. Visible security signage serves as a deterrent control as it discourages potential perpetrators by signaling the risk of detection and consequences, even if actual surveillance might not be active at all times.

Option A is incorrect. Encrypting all stored data is a preventive control that ensures unauthorized individuals cannot access or understand the encrypted information. It doesn't deter acts of physical vandalism.

Option B is incorrect. Installing biometric access controls is a preventive control that restricts physical access based on unique biological attributes. While it prevents unauthorized access, it doesn't act as a visible deterrent to vandalism or other potential threats.

Option C is incorrect. Implementing regular data backups is a corrective control designed to restore data after a security incident. It doesn't deter potential threats.

Question 49. Alice wants to access a restricted online portal. The portal asks her to enter a unique username and a secret passphrase only she should know. This process helps the system ensure that Alice is who she claims to be. What security concept is the portal employing?

- (A) Authorization
- (B) Accounting
- (C) Multifactor authentication
- (D) **Authentication**

Explanation 49. Correct Answer: D. Authentication.

Authentication is the process of verifying the identity of a user, system, or application. In the described scenario, Alice is proving her identity to the system by providing a unique username and a passphrase, which are credentials that supposedly only she possesses.

Option A is incorrect. Authorization determines what actions, resources, or services a verified identity is allowed to access or perform. It does not deal with verifying the identity itself.

Option B is incorrect. Accounting involves tracking user activities and recording them for audit purposes. It does not directly verify a user's identity.

Option C is incorrect. Multifactor authentication requires two or more methods of verification from different categories of

credentials. The scenario only mentioned a username and passphrase, which is a single-factor authentication method.

Question 50. Sophia, the cybersecurity lead at XYZ Corp, is in the process of drafting a new security policy. During the drafting process, she primarily consults with her security team. However, upon implementation, several departments pushed back due to the policy interfering with their operations. Which best describes the misstep Sophia made during the policy creation process?

- (A) Not using a standardized security framework
- (B) Over-reliance on automated security solutions
- (C) **Not including key stakeholders in the policy drafting process**
- (D) Focusing too much on external threats rather than internal ones

Explanation 50. Correct Answer: C. Not including key stakeholders in the policy drafting process. Stakeholders from different departments provide crucial insights into how security measures can impact various operations and processes within an organization. By including them in the policy drafting process, Sophia would have received feedback that could have helped shape a policy that not only maintains security but also aligns with the needs of different departments.

Option A is incorrect. While using a standardized security framework can provide guidance, it doesn't necessarily account for the unique operational needs of different departments within an organization.

Option B is incorrect. The scenario doesn't mention any reliance, over or otherwise, on automated security solutions.

Option D is incorrect. While both external and internal threats are crucial considerations, the primary issue here was the lack of consultation with key stakeholders.

Question 51. BioGen Inc., a biotechnology company, has implemented a layered security approach. They are considering adding a human element to their security measures for their research labs. Which of the following would best provide the ability to evaluate and respond to various security situations with human judgment?

- (A) Installing biometric locks
- (B) **Employing security guards**
- (C) Implementing an access control vestibule
- (D) Deploying AI-driven security cameras

Explanation 51. Correct Answer: B. Employing security guards. Security guards provide the advantage of human judgment and can evaluate, respond, and adapt to a wide variety of security situations, making them ideal for adding a human element to a layered security approach.

Option A is incorrect. While biometric locks can control access based on unique human features, they don't provide the evaluation and response capabilities of a human guard.

Option C is incorrect. An access control vestibule controls access into an area, often with two sets of doors, but it does not

provide the evaluation, judgment, or immediate response that a security guard does.

Option D is incorrect. While AI-driven security cameras can provide advanced monitoring and potentially detect suspicious activities, they don't replace the judgment and immediate response capabilities of a human security guard.

Question 52. While analyzing server logs, Mike, an IT security analyst, noticed that an unfamiliar document was frequently accessed. Upon investigation, he realized that this document was deliberately placed by the security team and had no real data but was closely monitored. The purpose of this file is MOST likely:

- (A) To serve as a redundancy copy in case of data loss
- (B) To act as a decoy to attract and detect unauthorized access**
- (C) To maintain a record of all user activities for auditing
- (D) To be encrypted and sent to clients as a sample

Explanation 52. Correct Answer: B. To act as a decoy to attract and detect unauthorized access. Honeyfiles serve as deceptive measures, attracting potential malicious actors or unauthorized users. If such files are accessed, it can be an indication of unauthorized or suspicious activities in the system.

Option A is incorrect. Redundancy copies or backups are created to prevent data loss due to unforeseen issues, but they are not monitored as decoys.

Option C is incorrect. User activity logs maintain records of actions taken within a system or application, which is different from a deceptive measure like a honeyfile.

Option D is incorrect. Files encrypted for client samples serve a different purpose and are not typically used as decoys to detect unauthorized access.

Question 53. DataCenter Inc. is located in a region prone to protests and vandalism. They wish to enhance their perimeter security to deter potential intruders and make it visibly clear that unauthorized access is restricted. Which of the following physical security measures would be the most effective first line of defense for the company?

- (A) Sliding Doors
- (B) Security Cameras
- (C) **High-security Fencing**
- (D) Proximity Card Readers

Explanation 53. Correct Answer: C. High-security Fencing. High-security fencing is a primary physical barrier that serves to deter, delay, and detect intrusions. It provides a clear visual indicator that delineates private property and can be equipped with additional deterrents such as barbed wire or sensors. Especially in areas prone to vandalism or protests, a robust fence acts as an immediate barrier to unauthorized access.

Option A is incorrect. Sliding doors are more applicable to internal security or entrance points and do not serve as a primary external barrier.

Option B is incorrect. While security cameras monitor and record activities, they do not serve as a physical barrier to prevent or deter unauthorized access.

Option D is incorrect. Proximity card readers are a form of access control that checks the credentials of individuals but do not serve as a primary deterrent against vandalism or protests.

Question 54. SecureTech Corp, a company dealing with sensitive client data, is redesigning its main office entrance to enhance security. They want to ensure that only one person gains access at a time, even if multiple people try to enter using a single authorized access badge. Which of the following would best serve this purpose?

- (A) CCTV Cameras
- (B) **Mantrap**
- (C) Biometric Scanners
- (D) Motion Detectors

Explanation 54. Correct Answer: B. Mantrap. A mantrap, also known as an access control vestibule, is a physical security access control system comprising a small space with two sets of interlocking doors. The first door must close before the second door opens, ensuring that only one person can pass through at a time. This design prevents tailgating or piggybacking, where unauthorized individuals attempt to enter a secure area by following closely behind an authorized individual.

Option A is incorrect. While CCTV cameras monitor and record activities, they do not physically prevent multiple people from entering at once using a single access badge.

Option C is incorrect. Biometric scanners provide a means of authenticating individuals based on unique physical or behavioral characteristics, but they do not prevent tailgating on their own.

Option D is incorrect. Motion detectors can detect movement but do not restrict the entry of multiple individuals trying to use a single authorized access badge.

Question 55. While setting up a new internal web application, Laura, a system administrator, decides to use a digital certificate for SSL/TLS encryption. Due to budget constraints, she can't procure a certificate from a commercial Certificate Authority (CA). Which of the following would be a viable option for Laura to secure the application?

- (A) Rely on plaintext HTTP for the application
- (B) Obtain a certificate from a free Certificate Authority
- (C) **Generate a self-signed certificate**
- (D) Use a shared certificate from another application

Explanation 55. Correct Answer: C. Generate a self-signed certificate. A self-signed certificate can be generated by Laura without the need for a Certificate Authority. While self-signed certificates can cause trust issues in public-facing applications (since they aren't signed by a recognized CA), they can be appropriate for internal applications where users can be informed and trust can be established manually.

Option A is incorrect. Relying on plaintext HTTP doesn't provide any encryption or security for the application, leaving it vulnerable to various attacks.

Option B is incorrect. While obtaining a certificate from a free Certificate Authority is a valid option, it wasn't the best choice given the specific scenario which emphasizes not using a CA.

Option D is incorrect. Using a shared certificate from another application can introduce security risks and is not a recommended practice.

Question 56. A network administrator has received a new security patch for a mission-critical application. Which of the following is the BEST action to take before applying this patch in the live environment?

- (A) Apply the patch immediately to ensure system security
- (B) Notify all users about the upcoming downtime due to the patch
- (C) **Test the patch in a separate testing environment**
- (D) Take a backup of only the mission-critical application

Explanation 56. Correct Answer: C. Test the patch in a separate testing environment. Testing any changes, including patches, in a separate environment before deploying them to production is essential to ensure there are no unintended technical implications. This is a key aspect of change management processes and helps prevent system outages or vulnerabilities from being introduced.

Option A is incorrect. While applying patches is crucial for maintaining security, doing so immediately without proper testing can lead to unforeseen technical problems.

Option B is incorrect. Notifying users is important, but it's premature to notify them without first testing the patch.

Option D is incorrect. Taking a backup is a good practice, but it is not a substitute for testing the patch first.

Question 57. After implementing a major security update to its database system, TechCo experienced unexpected downtime and system incompatibilities. The CISO wants to ensure that such incidents can be quickly addressed in the future. Which of the following should TechCo have had in place before deploying the update to mitigate the impact of these kinds of incidents?

- (A) A comprehensive list of all updates
- (B) An automated system recovery tool
- (C) **A backout plan**
- (D) A detailed user manual for the update

Explanation 57. Correct Answer: C. A backout plan. A backout plan is a pre-arranged strategy or set of procedures to reverse changes made to the system in case the changes have adverse effects. In scenarios like this, where a significant update causes unintended problems, a backout plan would allow the organization to revert the system to its previous stable state quickly.

Option A is incorrect. While having a comprehensive list of all updates is good for documentation and auditing purposes, it would not directly help in mitigating the effects of an adverse update.

Option B is incorrect. An automated system recovery tool might assist in reverting changes or recovering the system. However, a backout plan is more specific to undoing changes made during an update or change process, making it more suitable in this context.

Option D is incorrect. A detailed user manual for the update is beneficial for training and troubleshooting, but it wouldn't serve the direct purpose of reverting unintended adverse changes.

Question 58. A financial institution processes thousands of credit card transactions daily. To ensure the security and integrity of these transactions, the security officer wants to employ a solution that will safely manage and store cryptographic keys. Which of the following would be the MOST suitable solution?

- (A) Trusted Platform Module (TPM)
- (B) Full Disk Encryption (FDE)
- (C) **Hardware Security Module (HSM)**
- (D) Software Key Repository

Explanation 58. Correct Answer: C. Hardware Security Module (HSM). Hardware Security Modules (HSMs) are physical devices specifically designed to manage, process, and store cryptographic keys. They provide a high level of protection against both physical and logical attacks and are commonly used by financial institutions to ensure the security of high-value transactions.

Option A is incorrect. While TPMs provide hardware-level security for individual devices, they are not designed for the

high-capacity cryptographic needs of an institution processing numerous transactions.

Option B is incorrect. Full Disk Encryption (FDE) secures data at rest on a hard drive but doesn't specifically manage cryptographic keys used in transaction processing.

Option D is incorrect. While a software key repository can store cryptographic keys, it lacks the same level of physical and logical protection provided by an HSM.

Question 59. During the setup of a secure communication channel, Alice and Bob need to agree upon a shared secret key without sending the key directly to each other, as they fear eavesdropping. Which protocol would best facilitate this requirement?

- (A) RSA
- (B) HMAC
- (C) **Diffie-Hellman**
- (D) AES

Explanation 59. Correct Answer: C. Diffie-Hellman. The Diffie-Hellman key exchange protocol allows two parties to each generate public and private key pairs, exchange the public keys, and then derive a shared secret key. This secret key can then be used for symmetric encryption. The beauty of this protocol is that the shared secret can be derived without directly sending it over the communication channel, preventing eavesdroppers from obtaining the secret key directly.

Option A is incorrect. RSA is an asymmetric encryption method, not a key exchange protocol.

Option B is incorrect. HMAC is a specific type of message authentication code that involves hashing and is not used for key exchange.

Option D is incorrect. AES is a symmetric encryption algorithm and does not offer a key exchange mechanism.

Question 60. A company is developing a new video conferencing tool. They want to make sure that all video and audio data transmitted between participants are encrypted and protected from eavesdropping. Which type of encryption should the developers implement to achieve this?

- (A) Endpoint Encryption
- (B) **Transport-layer Encryption**
- (C) Volume-level Encryption
- (D) Database-level EncryptionAccess Control

Explanation 60. Correct Answer: B. Transport-layer Encryption. Transport-layer Encryption is tailored for securing data while it's in transit. By implementing this encryption, the company ensures that all video and audio data during the video conference are confidential, maintaining the privacy of the participants.

Option A is incorrect. Endpoint Encryption is designed for data on specific devices like laptops or mobile phones, not for data being transmitted over networks.

Option C is incorrect. Volume-level Encryption pertains to encrypting specific logical drives or volumes, not data in transit.

Option D is incorrect. Database-level Encryption secures data within a database and is not specific to data transmission over networks.

Question 61. After a significant cybersecurity incident, ABC Tech revamped its incident response procedures. However, the documentation was not updated to reflect these changes. During a subsequent minor incident, there was confusion regarding the steps to be followed. Which of the following is the MOST direct implication of not updating the incident response documentation?

- (A) The company may have to invest in new cybersecurity tools
- (B) Stakeholders might lose trust in the company's ability to handle incidents
- (C) **Incident response might be inconsistent and less effective**
- (D) ABC Tech may have to hire external consultants for incident response

Explanation 61. Correct Answer: C. Incident response might be inconsistent and less effective. Without up-to-date documentation reflecting the most recent incident response procedures, there's a risk that the response will be inconsistent, leading to inefficiencies and potential oversights.

Option A is incorrect. While new tools might be beneficial, the direct concern with outdated documentation is the effectiveness of the response.

Option B is incorrect. While stakeholder trust is important, the immediate implication of outdated documentation is the quality of the incident response.

Option D is incorrect. Hiring external consultants might be an option, but the direct consequence of outdated documentation is the potential ineffectiveness of the internal response process.

Question 62. A financial organization is considering implementing a system that allows all users to view all transactions, but once a transaction is recorded, it cannot be altered or deleted. They want this transparency to foster trust among their users. Which of the following would best meet this requirement?

- (A) Digital certificate
- (B) **Open public ledger**
- (C) Symmetric encryption
- (D) Secure file transfer protocol

Explanation 62. Correct Answer: B. Open public ledger. An open public ledger provides transparency by allowing all users to view all transactions. Moreover, once a transaction is added to the ledger, it becomes immutable, meaning it cannot be altered or deleted, ensuring data integrity and fostering trust among participants.

Option A is incorrect. A digital certificate is used to verify the identity of an entity and bind a public key to it, but it doesn't offer the transparency of transactions or their immutability.

Option C is incorrect. Symmetric encryption is used to encrypt and decrypt data using a single secret key, but it doesn't provide transaction transparency or immutability.

Option D is incorrect. Secure file transfer protocol (SFTP) is a method to securely transfer files over a network, but it doesn't maintain an open public ledger of transactions.

Question 63. A company is implementing a system to ensure that code released to production is both unaltered and approved by a specific team member. Which of the following cryptographic techniques should they implement?

- (A) Symmetric encryption of the code
- (B) Hashing the code with SHA-256
- (C) Encrypting the code with the team member's public key
- (D) **Digital signature by the team member**

Explanation 63. Correct Answer: D. Digital signature by the team member. Digital signatures provide both integrity and non-repudiation. By having the specific team member digitally sign the code, the company can ensure that the code has not been altered (integrity) and that it was approved by the designated individual (non-repudiation).

Option A is incorrect. Symmetric encryption provides confidentiality, but it doesn't provide the needed integrity and non-repudiation in this scenario.

Option B is incorrect. Hashing the code provides a mechanism to check for alterations (integrity), but it does not provide non-repudiation or evidence of the specific team member's approval.

Option C is incorrect. Encrypting with the team member's public key doesn't provide non-repudiation. Moreover, only the team member with the corresponding private key would be able to decrypt it, which might not be desirable for production releases.

Question 64. Your company has recently deployed an update to its CRM application. Post-update, users are experiencing connectivity issues. As a security administrator, which of the following steps should you take FIRST to address the connectivity problem without causing data loss?

- (A) Restart the application immediately
- (B) Disconnect all users and then restart the application
- (C) **Validate the update's integrity and then restart the application**
- (D) Reinstall the previous version of the CRM application

Explanation 64. Correct Answer: C. Validate the update's integrity and then restart the application. Before making any changes, it's essential to ensure the update's integrity. This means confirming that the update was correctly applied and that there were no issues during its installation. Once the update's integrity is confirmed, a restart can help apply any changes that may not have taken effect immediately.

Option A is incorrect. Restarting the application immediately without validation might cause further complications if the update was not correctly applied.

Option B is incorrect. While disconnecting users might be necessary at some point, doing so without validating the update's integrity can result in further disruptions.

Option D is incorrect. Reinstalling the previous version is a drastic step and might not be necessary if the update's integrity can be validated and issues resolved with a restart.

Question 65. TechDynamics, a growing tech startup, plans to scale its operations and serve a global clientele. Given that their client base operates in multiple time zones, when should TechDynamics schedule their system maintenance to ensure minimal disruption?

- (A) During the busiest hours for their headquarters' local time
- (B) Staggered based on the peak hours of their global clients
- (C) Only when a system breakdown occurs
- (D) **Establish a consistent maintenance window during off-peak hours for the majority of their clientele**

Explanation 65. Correct Answer: D. Establish a consistent maintenance window during off-peak hours for the majority of their clientele. When serving a global clientele operating in various time zones, it's crucial to establish a maintenance window during hours when the majority of clients are least active. This minimizes disruptions and ensures smooth operations for most clients.

Option A is incorrect. Focusing only on the headquarters' local time disregards the operational hours of global clients. This approach might cause disruptions for clients in other time zones.

Option B is incorrect. While staggering maintenance based on peak hours of global clients seems logical, it could lead to a complex and hard-to-manage maintenance schedule, especially as the client base grows.

Option C is incorrect. Waiting for a system breakdown to perform maintenance is reactive rather than proactive. This approach might lead to more extended and unpredictable downtimes, resulting in greater disruptions and potential security risks.

Question 66. During an IT audit, a company's encryption practices come under scrutiny. The IT auditor recommends increasing the encryption key length for certain applications to improve security. What is the PRIMARY reason to increase the encryption key length?

- (A) To speed up encryption and decryption processes
- (B) To ensure compatibility with older systems
- (C) **To reduce the possibility of a brute force attack**
- (D) To reduce the key management overhead

Explanation 66. Correct Answer: C. To reduce the possibility of a brute force attack. Increasing the encryption key length primarily enhances the security of the encryption by making it more resistant to brute-force attacks. A brute force attack involves trying all possible key combinations, and a

longer key length means exponentially more possible combinations, making the attack vastly more time-consuming and difficult.

Option A is incorrect. Longer key lengths generally slow down the encryption and decryption processes, as more computational power is required.

Option B is incorrect. Increasing key length might make the encryption incompatible with older systems that do not support the newer, longer key lengths.

Option D is incorrect. Key management overhead typically increases with longer key lengths, as more data must be managed and kept secure.

Question 67. Sarah is working on a project where she needs to validate the integrity and authenticity of assets over time, without a centralized authority. Which technology would be most appropriate for this use case?

- (A) Digital signature
- (B) Key escrow
- (C) **Blockchain**
- (D) Key management system

Explanation 67. Correct Answer: C. Blockchain. Blockchain technology allows for the validation of the integrity and authenticity of assets over time in a decentralized manner. Each transaction or asset is verified by the network's participants and added to the chain, ensuring its authenticity and making it tamper-evident.

Option A is incorrect. While digital signatures can validate the authenticity and integrity of a message or document, they do not provide a decentralized ledger of assets over time.

Option B is incorrect. Key escrow is a method where cryptographic keys are held in trust so that a third party can have access under certain conditions. It doesn't help in validating the integrity and authenticity of assets over time without central authority.

Option D is incorrect. A key management system manages the life cycle of cryptographic keys but does not inherently validate the integrity and authenticity of assets over time.

Question 68. A graphic design company frequently works with large files such as videos and high-resolution images. These files are stored on a dedicated storage volume in their server. While they need to secure this data, they don't want to encrypt individual files due to the volume of data and frequent access needs. Which encryption approach is most appropriate for this scenario?

- (A) File-level Encryption
- (B) Full-disk Encryption
- (C) Transport-layer Encryption
- (D) **Volume-level Encryption**

Explanation 68. Correct Answer: D. Volume-level Encryption. Volume-level Encryption allows the encryption of a specific volume or logical drive. In this case, it would allow the company to encrypt the entire volume where these large files are stored without having to encrypt individual files. This

ensures the entire volume's contents are encrypted while providing seamless access when required.

Option A is incorrect. File-level Encryption, while effective, would be tedious for encrypting numerous large files individually.

Option B is incorrect. Full-disk Encryption would encrypt the entire disk, which may not be necessary if only a specific volume requires encryption.

Option C is incorrect. Transport-layer Encryption pertains to data in transit and doesn't address the need of encrypting stored data at the volume level.

Question 69. An e-commerce company stores millions of customer transaction records in their primary database. They have decided to enhance their security posture by applying encryption to protect sensitive data. However, they don't want to encrypt the entire server storage, just the data within the database. Which encryption approach should the company adopt to meet their objective?

- (A) Full-disk Encryption
- (B) File-level Encryption
- (C) Volume-level Encryption
- (D) **Database-level Encryption**

Explanation 69. Correct Answer: D. Database-level Encryption. Database-level Encryption provides encryption

specifically for data within a database. It ensures that the data remains encrypted even when backed up, replicated, or moved. This approach is ideal for the e-commerce company as it focuses on encrypting the sensitive transaction records without affecting other data on the server.

Option A is incorrect. Full-disk Encryption would encrypt the entire server's storage, which may not be required by the company.

Option B is incorrect. File-level Encryption would require encrypting individual files, which may not be efficient for a database with millions of records.

Option C is incorrect. Volume-level Encryption encrypts specific volumes or logical drives, not just the database data.

Question 70. Your organization plans to upgrade its database system. To maintain security during this process, which of the following actions should be RESTRICTED until the upgrade is validated?

- (A) Monitoring the database for any anomalies
- (B) **Allowing end-users to access the upgraded database**
- (C) Making regular backups of the database
- (D) Reviewing the database system logs

Explanation 70. Correct Answer: B. Allowing end-users to access the upgraded database. Until the upgraded system is validated and any potential issues are addressed, end-user access should be restricted. This ensures that any vulnerabilities

or problems introduced by the upgrade don't compromise data or allow unauthorized activities.

Option A is incorrect. Monitoring the database is crucial to identify any potential security issues and should not be restricted.

Option C is incorrect. Regular backups should continue, as they are part of a comprehensive disaster recovery and data protection strategy.

Option D is incorrect. Reviewing logs is essential to monitor the system's health and security; hence, it should not be restricted.

Question 71. A journalist wants to send a confidential message to her editor without raising suspicion. Instead of sending a coded or encrypted text, she embeds the message within a harmless-looking photograph. What method is she employing to keep the message concealed?

- (A) Digital signature
- (B) Tunneling
- (C) **Steganography**
- (D) Chaining

Explanation 71. Correct Answer: C. Steganography.

Steganography is a technique used to conceal data within another piece of data. In this scenario, the journalist is embedding a confidential message within a photograph, making it look harmless and unsuspecting.

Option A is incorrect. A digital signature is used to verify the authenticity and integrity of a message or document. It doesn't hide information within another piece of data.

Option B is incorrect. Tunneling is a method used to encapsulate one protocol within another, typically used in VPNs to transport data over a public network.

Option D is incorrect. Chaining in the context of cryptography often refers to modes of operation like Cipher Block Chaining (CBC). It doesn't involve hiding data within other data.

Question 72. A security administrator needs to apply a configuration change to a critical service, requiring a service restart. Before initiating the restart, which of the following steps is MOST important to ensure continuous service availability?

- (A) **Implement automatic service restart on failure**
- (B) Announce the restart to all company employees
- (C) Schedule the restart during off-peak hours
- (D) Take a backup of the current service configuration

Explanation 72. Correct Answer: A. Implement automatic service restart on failure. Having an automatic service restart on failure ensures that if any issues arise after applying the configuration change, the service will attempt to restart itself, ensuring minimal interruption to its availability.

Option B is incorrect. While notifying company employees is good practice, it doesn't directly ensure continuous service availability.

Option C is incorrect. Scheduling during off-peak hours minimizes impact but doesn't ensure the service will be available if issues arise post-restart.

Option D is incorrect. While taking a backup of the configuration is crucial for rollback purposes, it doesn't ensure the service will remain available immediately post-restart.

Question 73. A security analyst at DataCorp is tasked with preventing unauthorized external applications from connecting to their server. Which approach should the analyst primarily rely on to achieve this?

- (A) **Implement an allow list for approved applications**
- (B) Monitor server CPU usage
- (C) Regularly patch server software
- (D) Encrypt data at rest on the server

Explanation 73. Correct Answer: A. Implement an allow list for approved applications. By implementing an allow list, the analyst can specify which applications are authorized to connect to the server. Any application not on the list will be prevented from establishing a connection, effectively stopping unauthorized external applications.

Option B is incorrect. While monitoring server CPU usage can provide insights into the server's performance and potential anomalies, it doesn't prevent unauthorized applications from connecting.

Option C is incorrect. Regularly patching server software is a best practice for security to fix known vulnerabilities. However,

patching doesn't directly prevent specific external applications from connecting.

Option D is incorrect. Encrypting data at rest helps protect stored data from unauthorized access but does not regulate which applications can connect to the server.

Question 74. Alice needs to provide proof of the authenticity of a digital document she's sending to Bob. Which of the following cryptographic elements should Alice use to accomplish this task and ensure Bob knows the document came from her?

- (A) Encrypt the document with Bob's private key
- (B) Encrypt the document with her public key
- (C) **Sign the document with her private key**
- (D) Sign the document with Bob's public key

Explanation 74. Correct Answer: C. Sign the document with her private key. To prove authenticity, a digital signature is created using the sender's private key. When Bob receives the document, he can verify the signature using Alice's public key. This proves that the document was signed by Alice and has not been tampered with during transit.

Option A is incorrect. Bob's private key is known only to Bob and should never be used by anyone else, including for encryption.

Option B is incorrect. Encrypting with Alice's public key doesn't prove authenticity. It would also mean only Alice's private key could decrypt it, which isn't the intent.

Option D is incorrect. One does not sign documents with the recipient's public key. Signatures are created using the sender's private key.

Question 75. Carla, a security analyst, receives an alert that one of the company's server certificates may have been exposed in a recent data breach. What is the most immediate action Carla should take to ensure that the exposed certificate cannot be used maliciously?

- (A) Request a new certificate from the CA
- (B) Update the company firewall rules
- (C) **Add the certificate to the Certificate revocation list (CRL)**
- (D) Perform a vulnerability assessment on the server

Explanation 75. Correct Answer: C. Add the certificate to the Certificate revocation list (CRL). If a certificate is believed to be compromised, the most immediate action is to revoke it. This is done by adding the certificate to the Certificate revocation list (CRL). Systems and applications that check the CRL before establishing secure communications will then know not to trust the compromised certificate.

Option A is incorrect. While requesting a new certificate may be necessary after revoking the compromised one, the immediate action should be revoking the potentially compromised certificate.

Option B is incorrect. Updating firewall rules, while essential for many security scenarios, doesn't directly address the misuse of a potentially exposed certificate.

Option D is incorrect. A vulnerability assessment is a broader action to identify weaknesses in the system. While valuable, it doesn't directly address the issue of the compromised certificate.

Question 76. A database administrator is concerned about identical hashes being produced for users who select the same password. To mitigate this risk, what cryptographic technique should the administrator implement?

- (A) Digital signature
- (B) **Salting**
- (C) Key stretching
- (D) Symmetric encryption

Explanation 76. Correct Answer: B. Salting. Salting involves adding a random value to a password before hashing it. This ensures that even if two users have the same password, their hashes will be different because of the unique salts. This makes it difficult for attackers to use precomputed tables (like rainbow tables) to match hashes to possible plaintext passwords.

Option A is incorrect. Digital signatures are primarily used to ensure the authenticity and integrity of a message or data, not for hashing passwords.

Option C is incorrect. Key stretching involves repeating the hashing process multiple times to make brute-force attacks more challenging, but it doesn't address the problem of identical hashes for identical passwords.

Option D is incorrect. Symmetric encryption uses the same key for both encryption and decryption and isn't related to the scenario of producing unique hashes for passwords.

Question 77. An online retailer is considering various methods to protect its customers' credit card information. Instead of storing the actual credit card numbers in their database, they opt for a solution that replaces the numbers with unrelated, random values. What is this method called?

- (A) Symmetric encryption
- (B) Digital watermarking
- (C) Hashing
- (D) **Tokenization**

Explanation 77. Correct Answer: D. Tokenization.

Tokenization is a method where sensitive data is replaced with non-sensitive substitutes, referred to as "tokens". These tokens act as references to the original data but don't contain the actual sensitive data, making it a preferred method for protecting credit card information in many retail environments.

Option A is incorrect. Symmetric encryption is a method of encrypting data using a single key for both encryption and decryption. It changes the original data into a ciphered format but doesn't replace it with random values as tokenization does.

Option B is incorrect. Digital watermarking embeds data into a digital signal, primarily for asserting rights or ownership and not for replacing sensitive data with random values.

Option C is incorrect. Hashing converts input data into a fixed-length string of characters, which is typically a hash code. It doesn't produce a random value that can be used as a reference back to the original data.

Question 78. During a scheduled maintenance window, a security administrator plans to apply a critical update to the company's firewall. Which of the following actions is MOST crucial to ensure minimized downtime during this process?

- (A) Notifying the firewall vendor about the update
- (B) Disabling all firewall rules temporarily
- (C) **Creating a rollback plan in case of update failure**
- (D) Scheduling the update during peak business hours

Explanation 78. Correct Answer: C. Creating a rollback plan in case of update failure. In change management processes, having a rollback plan ensures that if there are issues with the applied update, the system can be reverted to its previous state, thereby minimizing downtime.

Option A is incorrect. While it might be useful to notify the firewall vendor, it is not the most crucial step to minimize downtime.

Option B is incorrect. Disabling all firewall rules can introduce significant security risks and might not be related directly to the downtime.

Option D is incorrect. Scheduling updates during peak business hours could result in maximum disruption and downtime.

Question 79. A security administrator is considering a cryptographic solution for protecting data in transit between two servers located in the same data center. The primary goal is to ensure speed and efficiency in encryption and decryption processes. Which type of encryption would best meet this requirement?

- (A) Asymmetric encryption using RSA
- (B) **Symmetric encryption using AES**
- (C) Hybrid encryption using a combination of RSA and AES
- (D) Asymmetric encryption using ECC

Explanation 79. Correct Answer: B. Symmetric encryption using AES. Symmetric encryption, such as AES, is typically faster and requires less computational resources than asymmetric encryption. This makes it suitable for scenarios where high-speed encryption and decryption are essential, like for data in transit between servers in a data center.

Option A is incorrect. Asymmetric encryption using RSA is more computationally intensive than symmetric encryption and may not be the most efficient for the given scenario.

Option C is incorrect. While hybrid encryption can provide a balance of security and speed, using only symmetric encryption (AES) is more efficient for the described use case.

Option D is incorrect. ECC, like RSA, is an asymmetric encryption method, which means it will typically be slower than symmetric methods like AES.

Question 80. A software developer wants to store user passwords in a way that even if the database is compromised, attackers would not be able to retrieve the original passwords. What technique should the developer use to achieve this?

- (A) Symmetric encryption
- (B) Digital signing
- (C) **Hashing**
- (D) Steganography

Explanation 80. Correct Answer: C. Hashing. Hashing is a technique that takes an input (or ‘message’) and returns a fixed-size string of bytes, usually in the form of a digest. The output should ideally be unique (within reason) for every different input. It’s often used for storing passwords because even a tiny change in input will produce a dramatically different output, and it’s computationally hard to reverse the process.

Option A is incorrect. Symmetric encryption uses the same key for both encryption and decryption. If an attacker gains access to the encryption key, they can decrypt any encrypted data.

Option B is incorrect. Digital signing is used to verify the integrity and authenticity of a message but does not hide the original content.

Option D is incorrect. Steganography involves hiding information within other information, which isn’t related to securely storing passwords.

Question 81. A software development company is working on a mobile banking application. They want to ensure that sensitive

operations like cryptographic processes and biometric data validation are isolated from the main operating system to prevent potential tampering. Which tool should they consider implementing to achieve this objective?

- (A) Hardware Security Module (HSM)
- (B) Key Management System (KMS)
- (C) **Secure enclave**
- (D) Trusted Platform Module (TPM)

Explanation 81. Correct Answer: C. Secure enclave. A secure enclave is a hardware-based isolated environment often found in modern CPUs, especially in mobile devices. It's designed to run specific operations such as cryptographic processes and biometric data validation, ensuring that this data is kept isolated from the main operating system, making it resilient to tampering.

Option A is incorrect. While an HSM is a dedicated hardware device that manages cryptographic keys, it doesn't provide the isolated environment within a CPU for operations like the secure enclave does.

Option B is incorrect. KMS is primarily focused on the management of cryptographic keys, not on creating isolated environments for operations.

Option D is incorrect. TPM provides hardware-level security for individual devices, but it doesn't create a segregated environment within the CPU for operations like the secure enclave.

Question 82. A web server hosting the company's e-commerce site is set for an OS upgrade. The upgrade is expected to last 30 minutes. What should be a primary consideration to minimize customer impact due to potential downtime?

- (A) **Implementing a load balancer**
- (B) Taking a backup of the e-commerce site
- (C) Posting a maintenance notice a week in advance
- (D) Upgrading the server's hardware

Explanation 82. Correct Answer: A. Implementing a load balancer. A load balancer can redirect traffic to other servers while one is undergoing maintenance, ensuring that customers can still access the e-commerce site and minimizing the impact of downtime. Load balancers distribute incoming traffic across multiple servers, allowing one server to be taken offline without affecting the availability of the service.

Option B is incorrect. While backups are crucial for disaster recovery, they don't minimize immediate downtime during upgrades.

Option C is incorrect. While informing customers is a good practice, it doesn't prevent downtime. Some customers may still try to access the site during maintenance.

Option D is incorrect. Upgrading the server's hardware might improve performance but doesn't directly minimize the downtime caused by an OS upgrade.

Question 83. A project manager is working on a new product launch and has documents with sensitive financial projections

on her local computer. She occasionally shares these documents with select board members via email. While she wants to keep the financial documents secure, she doesn't want to encrypt all the data on her computer. Which encryption approach should she utilize?

- (A) Full-disk Encryption
- (B) Transport-layer Encryption
- (C) **File-level Encryption**
- (D) Partition Encryption

Explanation 83. Correct Answer: C. File-level Encryption.

File-level Encryption allows individual files or folders to be encrypted. In this scenario, the project manager can encrypt only the sensitive financial documents, allowing her to securely share them while keeping the rest of her data unencrypted.

Option A is incorrect. Full-disk Encryption would encrypt the entire drive, which is more than what's required.

Option B is incorrect. Transport-layer Encryption protects data in transit, but does not specifically address encrypting individual files for storage and sharing.

Option D is incorrect. Partition Encryption encrypts entire partitions or volumes, which isn't necessary in this scenario.

Question 84. A security analyst is evaluating security enhancements for a series of laptops that will store highly confidential data. The analyst wants to ensure that stored data remains encrypted and the integrity of the boot process is maintained. Which of the following would BEST meet this

requirement?

- (A) Installing antivirus software on each laptop
- (B) Enabling a software-based full-disk encryption
- (C) Implementing a BIOS password
- (D) Utilizing a Trusted Platform Module (TPM)

Explanation 84. Correct Answer: D. Utilizing a Trusted Platform Module (TPM). A Trusted Platform Module (TPM) is a specialized chip on an endpoint device that stores RSA encryption keys specific to the host system. It provides hardware-based security to enhance the security of the device by enabling features like hardware-based encryption and ensuring the integrity of the boot process, among other things.

Option A is incorrect. While antivirus software is vital for protecting against malware, it does not directly address hardware-based encryption or boot process integrity.

Option B is incorrect. Software-based full-disk encryption can ensure the confidentiality of data, but it does not offer hardware-level protection or boot process integrity like a TPM.

Option C is incorrect. A BIOS password provides a layer of security, but it does not offer encryption for stored data or ensure boot process integrity.

Question 85. A large e-commerce company is deploying a new online payment system. The Chief Information Security Officer (CISO) is concerned about the security of cryptographic keys and wants to ensure they are protected from potential theft or compromise. Which tool should the CISO implement to provide

the HIGHEST level of security for these keys?

- (A) Password vault
- (B) Software-based key storage
- (C) **Hardware Security Module (HSM)**
- (D) Cloud-based encryption service

Explanation 85. Correct Answer: C. Hardware Security Module (HSM). A Hardware Security Module (HSM) is a specialized device specifically designed to manage, protect, and securely store cryptographic keys. It is built to be tamper-resistant and provides a high level of security, making it suitable for environments where the protection of cryptographic keys is of paramount importance, such as in an e-commerce payment system.

Option A is incorrect. A password vault is designed primarily for storing and managing passwords, not cryptographic keys used in payment systems.

Option B is incorrect. Software-based key storage solutions do not provide the same level of physical security that an HSM offers.

Option D is incorrect. While cloud-based encryption services can provide encryption capabilities, they might not offer the same level of physical protection and control as an on-premises HSM.

Question 86. Sarah, a security analyst, is concerned about potential man-in-the-middle attacks on the company's internal portal. To mitigate this risk, she recommends obtaining a digital

certificate from a trusted entity. Which of the following is responsible for issuing such certificates?

- (A) Key distribution center
- (B) **Certificate authority (CA)**
- (C) Tokenization system
- (D) Security incident event manager

Explanation 86. Correct Answer: B. Certificate authority (CA). Certificate authorities (CAs) are trusted entities responsible for issuing, validating, and revoking digital certificates. These certificates are used to authenticate entities on the internet, such as websites, ensuring secure and authenticated communications, thus mitigating the risk of man-in-the-middle attacks.

Option A is incorrect. A Key distribution center (KDC) is a part of the Kerberos authentication protocol and is responsible for distributing session tickets and temporary session keys, not for issuing digital certificates.

Option C is incorrect. Tokenization systems replace sensitive data with non-sensitive substitutes, known as tokens. They don't issue digital certificates.

Option D is incorrect. A Security incident event manager (SIEM) aggregates and analyzes log data from various sources, providing real-time analysis of security alerts, but does not issue certificates.

Question 87. A financial institution is looking to adopt an encryption algorithm for its transactions that is considered to be

very secure due to its longer key length, compared to older standards. Which encryption algorithm best fits this description?

- (A) DES
- (B) Blowfish
- (C) RSA
- (D) **AES-256**

Explanation 87. Correct Answer: D. AES-256. AES-256, part of the Advanced Encryption Standard (AES) family, utilizes a 256-bit key length. This extended key length provides a higher degree of security and is considered resistant to all known practical attacks when used properly.

Option A is incorrect. DES (Data Encryption Standard) has a key length of only 56 bits and is considered to be insecure against sufficiently equipped attackers due to its shorter key length.

Option B is incorrect. While Blowfish is a symmetric encryption algorithm, it's older and not as universally recommended for secure transactions as AES.

Option C is incorrect. RSA is an asymmetric encryption algorithm, not typically used directly for encrypting bulk transaction data.

Question 88. Alice receives an email from Bob with an attached document. She wants to verify both the authenticity of the sender and the integrity of the attached document. Which of the following should Bob have used before sending the email?

- (A) Encrypt the document with his private key

- (B) Hash the document
- (C) Encrypt the document with Alice's public key
- (D) **Sign the document with his private key**

Explanation 88. Correct Answer: D. Sign the document with his private key. Digital signatures are created by taking a hash of a message (or document) and then encrypting that hash with the sender's private key. When Alice receives the email, she can decrypt the signature using Bob's public key to retrieve the original hash and then compare it with her computed hash of the document. If they match, it confirms both the sender's identity (authenticity) and that the document has not been altered (integrity).

Option A is incorrect. Encrypting the entire document with his private key isn't practical for verifying authenticity and integrity. Instead, the hash of the document is encrypted to create a signature.

Option B is incorrect. Simply hashing the document will provide a way to check the document's integrity but does not verify the authenticity of the sender.

Option C is incorrect. Encrypting the document with Alice's public key would make it confidential for Alice, but this doesn't help in verifying authenticity or integrity.

Question 89. During a critical financial quarter, GlobalFin Corp experienced unexpected outages during peak business hours due to system maintenance, impacting its operations significantly. To prevent such occurrences in the future, what should

GlobalFin Corp implement regarding their maintenance activities?

- (A) Conduct maintenance activities randomly to avoid predictability
- (B) Implement maintenance activities during peak business hours
- (C) **Establish designated maintenance windows**
- (D) Reduce the frequency of maintenance activities

Explanation 89. Correct Answer: C. Establish designated maintenance windows. Maintenance windows are specific time frames designated for system maintenance, ensuring that disruptions due to updates, patches, or other maintenance activities don't occur during critical business hours. By setting these windows, usually during off-peak times, businesses can minimize operational disruptions.

Option A is incorrect. Conducting maintenance activities randomly can lead to unpredictable outages, which can be disruptive to business operations and degrade trust among stakeholders.

Option B is incorrect. Implementing maintenance activities during peak business hours is precisely what led to the disruption in the scenario. This approach would likely cause more operational problems, especially for businesses with critical operations during these hours.

Option D is incorrect. Reducing the frequency of maintenance activities might decrease disruptions, but it could also lead to

unpatched vulnerabilities, outdated software, or other security and operational issues.

Question 90. A financial institution wants to securely transfer transaction data between its main office and a branch office. The data should be encrypted while in transit to prevent any interception and unauthorized access. Which encryption solution is most suitable for securing the data during transport?

- (A) Database-level Encryption
- (B) Full-disk Encryption
- (C) **Transport-layer Encryption**
- (D) File-level Encryption

Explanation 90. Correct Answer: C. Transport-layer Encryption. Transport-layer Encryption is specifically designed to protect data while it is in transit over a network. It ensures that the data remains confidential and is not tampered with during transmission. For the financial institution, this approach would be most effective in securing the transaction data between offices.

Option A is incorrect. Database-level Encryption is used to secure data stored within a database, not for data in transit.

Option B is incorrect. Full-disk Encryption secures the entire storage of a device and is not specific to data being transferred over a network.

Option D is incorrect. File-level Encryption encrypts individual files but may not ensure the confidentiality of the data while it's being transmitted over a network.

Question 91. After a recent software update, a company's intranet portal has been inaccessible to a few employees. The IT team suspects it could be due to network filtering rules. What should the IT team review to confirm their suspicions?

- (A) The content filtering policies
- (B) The malware detection logs
- (C) **The allow list/deny list configurations**
- (D) The network bandwidth utilization graphs

Explanation 91. Correct Answer: C. The allow list/deny list configurations. Network accessibility issues, especially after software or configuration changes, can often arise due to misconfigured allow lists or deny lists. Reviewing these configurations can help determine if specific IP addresses or domains have been incorrectly blocked or not allowed, causing the inaccessibility issues.

Option A is incorrect. Content filtering policies primarily focus on blocking specific types of content (like social media or adult sites) rather than causing inaccessibility to specific users or departments.

Option B is incorrect. Malware detection logs track potential security threats and not network access configurations. They wouldn't typically cause a selective inaccessibility issue unless a specific user's machine is quarantined.

Option D is incorrect. While network bandwidth utilization graphs might show reduced traffic, they won't provide details on specific allow/deny list configurations that might be causing the inaccessibility.

Question 92. A user wants to send a confidential email to their colleague and ensure that only the intended recipient can read it. The user also wants to provide assurance to the recipient that the email was indeed sent by them. Which encryption method should the user employ to accomplish this?

- (A) Use symmetric encryption with a shared key
- (B) Use asymmetric encryption and encrypt the email with the recipient's public key
- (C) Use asymmetric encryption, encrypt the email with the user's private key
- (D) Use asymmetric encryption, first sign the email with the user's private key, then encrypt it with the recipient's public key**

Explanation 92. Correct Answer: D. Use asymmetric encryption, first sign the email with the user's private key, then encrypt it with the recipient's public key.

Option D offers both confidentiality and non-repudiation.

The email is encrypted with the recipient's public key, ensuring only the recipient can decrypt it using their private key. Signing the email with the sender's private key allows the recipient to verify the sender using the sender's public key.

Option A is incorrect. While symmetric encryption provides confidentiality, it doesn't offer non-repudiation or sender verification.

Option B is incorrect. Encrypting with the recipient's public key provides confidentiality but lacks sender verification.

Option C is incorrect. Encrypting an email with the user's private key would offer sender verification but won't provide confidentiality.

Question 93. A user, Amy, wants to securely send a confidential document to her colleague, Bob. Amy decides to encrypt the document to ensure its confidentiality. Which of the following should Amy use to encrypt the document, ensuring only Bob can decrypt it?

- (A) Amy's private key
- (B) Amy's public key
- (C) Bob's private key
- (D) **Bob's public key**

Explanation 93. Correct Answer: D. Bob's public key. In asymmetric encryption, if a message is encrypted with an individual's public key, only the corresponding private key can decrypt it. Therefore, to ensure Bob is the only person who can decrypt the document, Amy should encrypt it using Bob's public key.

Option A is incorrect. Encrypting with Amy's private key would allow anyone with Amy's public key to decrypt it, and it would also serve as a digital signature rather than ensuring confidentiality.

Option B is incorrect. Using Amy's public key would not make sense because then only Amy's private key could decrypt it.

Option C is incorrect. The private key should never be shared or used for encryption. Its main use is for decryption and signing.

Question 94. A cybersecurity analyst is investigating a suspicious image file received via email. Upon closer examination, the analyst suspects that the image might be carrying hidden data because the file size is unusually large. Which technique might the sender have used to embed secret information within the image?

- (A) Symmetric encryption
- (B) Digital watermarking
- (C) **Steganography**
- (D) Hashing

Explanation 94. Correct Answer: C. Steganography.

Steganography is the practice of hiding information within another form of data. In this case, the analyst suspects that an image file is carrying hidden data due to its unusually large size, which is a common indicator of steganographic practices.

Option A is incorrect. Symmetric encryption is used for encrypting data using a single key for both encryption and decryption. It doesn't hide data within other data.

Option B is incorrect. Digital watermarking embeds information into a digital signal, but it's generally used to assert rights or ownership, not to hide data in the manner of steganography.

Option D is incorrect. Hashing is the process of converting an input into a fixed-length string of bytes, generally used to verify data integrity.

Question 95. A company is preparing to roll out a new infrastructure deployment for its internal network. They have a server that will store both highly confidential customer information and non-sensitive marketing material. The IT department wants to ensure that only the confidential data is encrypted, while the marketing data remains easily accessible. Which level of encryption would be most suitable for this scenario?

- (A) File-level Encryption
- (B) Full-disk Encryption
- (C) **Partition Encryption**
- (D) Transport-layer Encryption

Explanation 95. Correct Answer: C. Partition Encryption.

Partition Encryption allows specific partitions or volumes of a storage drive to be encrypted. By encrypting only the partition that contains confidential data, the company can ensure the security of sensitive information while leaving other partitions, such as the one with marketing material, unencrypted for easy access.

Option A is incorrect. File-level Encryption would require each confidential file to be encrypted individually, which could be cumbersome.

Option B is incorrect. Full-disk Encryption would encrypt the entire disk, including the non-sensitive marketing material.

Option D is incorrect. Transport-layer Encryption protects data in transit, not data at rest on storage drives.

Question 96. Sarah, a cybersecurity analyst, receives a report that a company laptop was stolen from an employee's car. The laptop contained sensitive financial data. Sarah checked the company's security configurations and found that the laptop was equipped with full-disk encryption. How does this impact the potential data breach situation?

- (A) The data remains easily accessible, as only the boot sector was encrypted
- (B) The data is protected, as the entire hard drive's contents are encrypted**
- (C) The data is partially encrypted, with only the user directories protected
- (D) The data is vulnerable since full-disk encryption only applies when the laptop is connected to the company network

Explanation 96. Correct Answer: B. The data is protected, as the entire hard drive's contents are encrypted. Full-disk Encryption (FDE) encrypts the entirety of a hard drive, ensuring that all its contents, including system and user files, are unreadable without the appropriate decryption key or credentials. As such, even if the laptop is stolen, the data remains secured unless the attacker has the decryption key.

Option A is incorrect. Full-disk Encryption does not encrypt only the boot sector; it encrypts the entire disk.

Option C is incorrect. Full-disk Encryption doesn't only encrypt user directories; it encrypts the whole disk.

Option D is incorrect. Full-disk Encryption protects the data at all times, irrespective of the laptop's connection to a network.

Question 97. A university's IT department provides access to its student records for training purposes to new hires. To protect student identities, they replace the real names and social security numbers with fictitious ones while maintaining the database's original format. Which technique is the IT department utilizing?

- (A) Digital signing
- (B) **Data masking**
- (C) Steganography
- (D) Data deduplication

Explanation 97. Correct Answer: B. Data masking. Data masking protects the data subject's data privacy by obscuring specific data within a database, making the data unreadable and unusable, especially in non-production environments. It is commonly used for testing and development purposes.

Option A is incorrect. Digital signing involves using a digital signature to prove the authenticity and integrity of data.

Option C is incorrect. Steganography involves hiding information within other information, such as embedding text within images, making it undetectable.

Option D is incorrect. Data deduplication is the process of eliminating duplicate copies of repeating data to save storage space.

Question 98. A company is looking for a cryptographic solution that provides an immutable and transparent record of all transactions in a distributed ledger system. Which of the following would BEST meet this requirement?

- (A) Symmetric key algorithm
- (B) Public key infrastructure
- (C) **Blockchain**
- (D) Digital watermark

Explanation 98. Correct Answer: C. Blockchain. Blockchain is a decentralized and distributed ledger technology that provides an immutable record of transactions. Each block contains a list of transactions and is linked to the previous block, creating a chain. The transparency and immutability of blockchain make it especially suitable for applications where an irrefutable record is essential.

Option A is incorrect. Symmetric key algorithms are encryption methods where the same key is used for both encryption and decryption but don't inherently provide an immutable record of transactions.

Option B is incorrect. Public key infrastructure (PKI) is used for digital certificates and keys distribution but doesn't offer an immutable record of transactions.

Option D is incorrect. Digital watermarking embeds information into a digital signal, but it doesn't provide an immutable record of transactions.

Question 99. An IT manager is considering solutions to protect data stored on the laptops provided to remote employees. The primary concern is to ensure that the entire content of the laptop's storage drive is unreadable if a laptop is lost or stolen. Which encryption level would best address this concern?

- (A) File-level Encryption
- (B) Transport-layer Encryption
- (C) **Full-disk Encryption**
- (D) Database-level Encryption

Explanation 99. Correct Answer: C. Full-disk Encryption.

Full-disk Encryption (FDE) encrypts the entire storage drive, making all data on the drive unreadable without the correct decryption key or credentials. This is especially useful for portable devices like laptops, which are more vulnerable to physical theft.

Option A is incorrect. File-level Encryption encrypts individual files rather than the entire disk, so some data or system files might remain unencrypted.

Option B is incorrect. Transport-layer Encryption protects data in transit, not data at rest on storage drives.

Option D is incorrect. Database-level Encryption encrypts data within a database and does not apply to other files or data outside of that database.

Question 100. The finance department at a large firm still relies on a legacy application for their quarterly reporting. This application is known to have some security flaws, but due to its

critical nature, it cannot be easily replaced. How can the firm BEST mitigate the risks associated with this application?

- (A) Train the finance team about the latest cybersecurity threats
- (B) Run the legacy application on the latest hardware to improve performance
- (C) **Place the legacy application behind a web application firewall (WAF)**
- (D) Frequently change the passwords of users who have access to the application

Explanation 100. Correct Answer: C. Place the legacy application behind a web application firewall (WAF). By placing the application behind a WAF, the firm can filter, monitor, and block malicious HTTP traffic targeting the application's vulnerabilities, thereby offering a layer of protection against potential security flaws in the legacy application.

Option A is incorrect. While training is essential, it doesn't directly address the vulnerabilities in the legacy application.

Option B is incorrect. Using the latest hardware might improve application performance but doesn't mitigate the security risks associated with its vulnerabilities.

Option D is incorrect. While frequent password changes can enhance security, they don't address the inherent vulnerabilities in the legacy application.

Question 101. A multinational corporation is concerned about the possibility of losing access to encrypted data due to the loss or compromise of private keys. They've approached a third-party organization for a solution. Which of the following is a system that allows the third party to securely hold a copy of the corporation's cryptographic keys to ensure data recoverability?

- (A) Public Key Repository
- (B) Key Generation Center
- (C) **Key Escrow**
- (D) Key Renewal Service

Explanation 101. Correct Answer: C. Key Escrow. Key escrow is a system in which cryptographic keys are securely stored with a third party, so they can be retrieved in cases where the original keys are lost or compromised. This ensures data recoverability while maintaining security.

Option A is incorrect. A Public Key Repository is where public keys are stored for retrieval, not for backup or recovery purposes.

Option B is incorrect. Key Generation Center is responsible for creating cryptographic keys, not storing them for recovery purposes.

Option D is incorrect. Key Renewal Service deals with replacing and updating cryptographic keys as they expire or need refreshing, not storing them for recovery.

Question 102. A financial institution plans to provide access to its database for third-party developers to create new

applications. However, they want to ensure that the developers do not see the actual data but instead work with a disguised version that retains the data's original structure. What technique is the financial institution considering?

- (A) Tokenization
- (B) **Data masking**
- (C) Encryption
- (D) Digital watermarking

Explanation 102. Correct Answer: B. Data masking. Data masking is a technique that obscures specific data within a database, making the data unreadable and unusable. The method is often employed in non-production environments to protect the data subject's data privacy and data security.

Option A is incorrect. Tokenization replaces sensitive data with random tokens, which act as references to the original data.

Option C is incorrect. Encryption converts readable data into an unreadable format to protect its confidentiality. It requires a key to return the data to its original form.

Option D is incorrect. Digital watermarking embeds data into a digital signal, primarily for asserting rights or ownership.

Question 103. NexTech, a cloud-based software company, recently faced a security breach due to inconsistent practices among its system administrators. To avoid such inconsistencies in the future, what should NexTech emphasize in its operations?

- (A) Rely on system administrators to develop their personal methods

- (B) Mandate frequent system reboots
- (C) **Implement Standard Operating Procedures (SOPs) for all technical operations**
- (D) Conduct random security audits without notifying administrators

Explanation 103. Correct Answer: C. Implement Standard Operating Procedures (SOPs) for all technical operations.

Standard Operating Procedures (SOPs) provide a consistent and documented process that employees can follow. By implementing SOPs, businesses ensure that tasks are performed uniformly, reducing the risk of errors and inconsistencies that might lead to security vulnerabilities.

Option A is incorrect. Relying on individual system administrators to develop their personal methods can lead to inconsistent practices and operational inefficiencies, increasing the risk of security breaches.

Option B is incorrect. Frequent system reboots, while they might be part of some SOPs, don't address the root issue of inconsistency among system administrators. It's the consistent method of operations that prevents errors, not just frequent restarts.

Option D is incorrect. While security audits are essential, conducting them without notice doesn't address the core issue of inconsistency in system administration practices.

Question 104. After a series of system enhancements, a financial organization decided to use a manual method of

documenting changes in separate files rather than implementing a version control system. During an audit, the cybersecurity team struggled to determine which version of a critical system file was the most recent and accurate. What is the PRIMARY risk of not implementing version control for such documentation?

- (A) Increased storage requirements for multiple files
- (B) Difficulty in collaborating between team members
- (C) **Lack of traceability and difficulty in reverting to a known stable state**
- (D) Greater need for training staff on manual documentation

Explanation 104. Correct Answer: C. Lack of traceability and difficulty in reverting to a known stable state. Version control provides a clear history of changes, ensuring easy reversion to a known stable state, and identifying the latest version of a document or system file. In the absence of version control, identifying the most recent and accurate version can be challenging.

Option A is incorrect. While storage might be a concern, the primary risk is the inability to trace changes and revert to a stable state.

Option B is incorrect. Collaboration might be hindered, but the direct risk is associated with traceability and stability.

Option D is incorrect. Training staff is always essential, but the immediate concern is the ability to trace and manage changes.

Question 105. During a security audit, it was found that an application was using plain hashes for storing passwords. The security team recommended a method that involves using the original password along with a salt and then rehashing it multiple times. What is this method known as?

- (A) Key clustering
- (B) Rainbow table prevention
- (C) Key rotation
- (D) **Key stretching**

Explanation 105. Correct Answer: D. Key stretching. Key stretching refers to the process of taking a password and, usually in combination with a salt, hashing it multiple times. This repeated hashing process makes brute-force attacks more time-consuming and difficult because the attacker has to not only guess the password but also apply the hashing function the same number of times the original process used.

Option A is incorrect. Key clustering pertains to different keys producing the same ciphertext from the same plaintext, which is not relevant to the described scenario.

Option B is incorrect. While using salts can prevent the effective use of rainbow tables, the act of rehashing passwords multiple times is not specifically called “rainbow table prevention.”

Option C is incorrect. Key rotation involves periodically changing cryptographic keys. It does not relate to hashing passwords multiple times.

Question 106. During a routine update, a web server application requires a restart. What should the administrator do FIRST to ensure client connections aren't abruptly terminated during the restart?

- (A) **Redirect incoming traffic to a backup server**
- (B) Increase the server's memory
- (C) Manually terminate all active client sessions
- (D) Check for available patches for the application

Explanation 106. Correct Answer: A. Redirect incoming traffic to a backup server. Redirecting incoming traffic ensures that clients are not abruptly disconnected and instead can continue their activities on a backup server while the primary server undergoes a restart.

Option B is incorrect. Increasing server memory might improve performance but doesn't address the immediate issue of the service restart.

Option C is incorrect. Manually terminating client sessions would cause abrupt disconnections, which is what the administrator is trying to avoid.

Option D is incorrect. While checking for patches is important, it doesn't address the issue of ensuring client connections aren't terminated during a service restart.

Question 107. Carlos is responsible for managing IT services for a university. The university has numerous departments, each with its subdomain, like arts.university.com, science.university.com, and sports.university.com. Carlos wants

a solution that ensures HTTPS security while being cost-effective. However, he's wary of potential risks. What might be a drawback of using a Wildcard Certificate for the university's subdomains?

- (A) It can secure only one subdomain
- (B) **If compromised, all subdomains are at risk**
- (C) It only validates the domain ownership, not the organization's identity
- (D) It's the most expensive certificate available

Explanation 107. Correct Answer: B. If compromised, all subdomains are at risk. The primary concern with a Wildcard Certificate is that if its private key is compromised, it jeopardizes the security of all associated subdomains. This poses a significant risk since the exposure of a single key could lead to potential attacks or misuse across all subdomains.

Option A is incorrect. A Wildcard Certificate can secure multiple subdomains under a single domain.

Option C is incorrect. While true for Domain Validated (DV) certificates, Wildcard Certificates can also be available with Organization Validation (OV), ensuring organizational identity.

Option D is incorrect. Wildcard Certificates aren't necessarily the most expensive. The cost varies based on the level of validation and the issuing authority.

Question 108. Your organization is preparing to upgrade a database server that supports an e-commerce application. A review of the change management documentation has revealed

that multiple applications rely on this particular database server for various functionalities. Which of the following steps should be taken FIRST to ensure a smooth upgrade process without disruptions?

- (A) Upgrade the database server immediately to benefit from new features
- (B) Perform a backup of the database server
- (C) **Identify and test all applications that have dependencies on the database server**
- (D) Inform users about potential downtime during the upgrade

Explanation 108. Correct Answer: C. Identify and test all applications that have dependencies on the database server.

Before making changes, especially to systems with multiple dependencies, it's crucial to understand the full scope of potential impacts. By identifying and testing all dependent applications, you ensure that the upgrade won't inadvertently disrupt other services or functionalities.

Option A is incorrect. Upgrading immediately without considering dependencies can lead to unforeseen disruptions and complications.

Option B is incorrect. While backing up the server is a good practice, understanding dependencies should come first to plan the upgrade effectively.

Option D is incorrect. Informing users is essential, but understanding the upgrade's potential impact should come first to provide accurate information.

Question 109. After a recent data breach, a multinational corporation is evaluating its cryptographic practices. The Chief Security Officer (CSO) determines that the manual management of cryptographic keys has become too complex due to the scale of the operations. Which tool would BEST address the CSO's concern while ensuring robust security practices?

- (A) Password Management System
- (B) Secure File Transfer Protocol (SFTP)
- (C) Trusted Platform Module (TPM)
- (D) **Key Management System (KMS)**

Explanation 109. Correct Answer: D. Key Management System (KMS). A Key Management System (KMS) is specifically designed to handle the generation, distribution, rotation, and retirement of cryptographic keys in a centralized and automated manner. For large organizations, using a KMS streamlines and secures the complex task of key management.

Option A is incorrect. While a Password Management System helps in handling and storing passwords, it does not provide comprehensive features needed for cryptographic key management.

Option B is incorrect. SFTP is a protocol for securely transferring files over a network, not for managing cryptographic keys.

Option C is incorrect. While TPM provides hardware-level security for individual devices, it is not meant for enterprise-wide key management.

Question 110. During a quarterly review, the IT team at a logistics company decided to change the configuration of their load balancers to better distribute traffic among their servers. After the change, a series of technical issues emerged, affecting customer-facing applications. When troubleshooting the issue, it was discovered that the network diagrams had not been updated to reflect the new changes. What is the MAJOR consequence of not having updated diagrams in such a scenario?

- (A) The servers might need a hardware upgrade
- (B) The company might need to revert to the old load balancer configuration
- (C) **It increases the time and complexity of troubleshooting**
- (D) Customers might prefer other logistics companies

Explanation 110. Correct Answer: C. It increases the time and complexity of troubleshooting. Accurate and up-to-date documentation, including network diagrams, is crucial for effective troubleshooting. Without it, IT teams can spend unnecessary time trying to understand the current state of the system, delaying the resolution of the issue.

Option A is incorrect. While server upgrades might be necessary in some cases, it's not a direct consequence of outdated diagrams.

Option B is incorrect. Reverting to an old configuration might be a potential solution, but the primary issue is the increased troubleshooting complexity due to outdated documentation.

Option D is incorrect. While the potential loss of customers can be an indirect consequence of prolonged technical issues, the immediate concern of outdated diagrams is the impact on troubleshooting.

CHAPTER 2

THREATS, VULNERABILITIES, AND MITIGATIONS

Questions 111-220

Question 111. A medium-sized company suffered a data breach. Investigations revealed that an attacker from a rival firm had exploited a misconfigured firewall to gain unauthorized access to the company's database. Based on the attributes of the actor, how would this threat actor be best described?

- (A) Internal actor leveraging physical access
- (B) Internal actor abusing privileges
- (C) External actor using social engineering
- (D) External actor exploiting technical vulnerabilities

Question 112. Sophia, the CFO of a medium-sized company, received a call from an individual claiming to be from the IT

department. The caller requested her login details for a “critical system update.” Suspecting something wasn’t right, Sophia hung up and contacted her IT department, which confirmed no such call was made by them. Which type of attack did Sophia most likely experience?

- (A) Vishing
- (B) Phishing
- (C) SQL Injection
- (D) Cross-Site Request Forgery (CSRF)

Question 113. During an incident response, the IT team discovers malware that collects information about military projects. The malware sends the data to a server located in a foreign country. Which type of threat actor would MOST likely be involved in this type of cyber espionage?

- (A) Disgruntled employee
- (B) Nation-state
- (C) Phishing scam artist
- (D) Hacktivist

Question 114. A company’s website was temporarily defaced with a humorous meme, but no sensitive data was stolen or any significant damage done. The attacker left a message bragging about their first successful hack. Which type of threat actor is MOST likely responsible for this attack?

- (A) Insider threat
- (B) Advanced Persistent Threat (APT)
- (C) Unskilled attacker
- (D) Nation-state

Question 115. A new technology firm recently launched a device that uses facial recognition for authentication. A cybersecurity researcher, without any malicious intent, demonstrated a method to bypass the facial recognition using a photograph. The researcher then approached the firm with the findings without publicizing it. What is the primary motivation behind the researcher's action?

- (A) Philosophical beliefs opposing facial recognition
- (B) Financial gain by blackmailing the firm
- (C) Ethical considerations for consumer security
- (D) Aiming to damage the firm's market reputation

Question 116. Mike, a network administrator, notices an unauthorized device connected directly to the company's main network switch in the server room. This device is attempting to capture network traffic. What kind of attack is this unauthorized device likely conducting?

- (A) Rogue access point
- (B) VLAN hopping
- (C) Port mirroring
- (D) ARP poisoning

Question 117. Alex, an employee at XYZ Corp, noticed an unfamiliar USB drive lying in the company parking lot. Out of curiosity, Alex plugged the device into his workstation. Almost immediately, his antivirus program detected malicious software trying to execute. What type of attack did Alex likely encounter?

- (A) Man-in-the-Middle Attack
- (B) Evil Twin

- (C) Spear Phishing
- (D) USB Drop Attack

Question 118. A company named TechFlow is planning to produce a new line of smart home devices. They have opted to use a single supplier for a crucial component in their devices. Which of the following represents the MOST significant security risk associated with this decision?

- (A) It will be challenging to negotiate prices with just one supplier
- (B) If the supplier's delivery timeline is delayed, product launch might be postponed
- (C) A compromise at the supplier could lead to vulnerabilities in all devices
- (D) TechFlow will need to rely on the supplier's warranty and return policies

Question 119. A high-profile executive received an email containing personal photos and a message threatening to release the images to the public unless a significant sum of money was transferred to a specific cryptocurrency address. What motivation is most evident behind this threat?

- (A) Espionage to gather competitive intelligence
- (B) Service disruption to harm the reputation of the executive's company
- (C) Blackmail to extract money by leveraging sensitive information
- (D) Data exfiltration for selling on the dark web

Question 120. Jane, an accountant in a multinational corporation, received an email from what seemed to be the

company's IT department. The email had the company's logo, colors, and font and urged Jane to click on a link to reset her password due to "suspicious activity." However, upon close inspection, Jane noticed a minor spelling error in the domain name of the sender's email address. What type of attack does this scenario describe?

- (A) Spear Phishing
- (B) Vishing
- (C) Baiting
- (D) Brand Impersonation

Question 121. During a routine scan, the security team at a graphic design firm discovers that an employee downloaded an image from an email and subsequently, unusual network traffic was detected originating from that employee's workstation. The image appeared normal when opened. What type of attack might have been used in this situation?

- (A) Image Steganography Malware
- (B) Password Brute Force
- (C) Phishing
- (D) Port Scanning

Question 122. Acme Corp, a large organization, has recently entered into a contract with Zenith MSP for IT management and support. The CISO of Acme Corp is concerned about the security risks associated with this new relationship. Which of the following is the PRIMARY security concern when utilizing managed service providers (MSPs) in a supply chain?

- (A) Increased costs due to the integration of new technologies
- (B) Difficulty in ensuring consistent patch management

- (C) Potential for unauthorized access to company resources
- (D) Decreased IT staff morale due to outsourcing

Question 123. Mike, an employee at a tech company, receives an instant message from a coworker named Jessica. The message contains a link and claims to showcase a hilarious video. However, Mike knows Jessica is on vacation. He suspects the message might not genuinely be from her. What type of threat is Mike most likely encountering?

- (A) Watering Hole Attack
- (B) Man-in-the-Middle Attack
- (C) IM Spoofing
- (D) Side-channel Attack

Question 124. During a political campaign, an anonymous group releases a series of articles containing fabricated data about a candidate's past, intending to influence voters' opinions. This is an example of:

- (A) Impersonation
- (B) SSmishing
- (C) Disinformation
- (D) Baiting

Question 125. Sophia received an email from her bank asking her to urgently update her personal details due to a system upgrade. The email contains a link that redirects to a website that looks similar to her bank's website. Which of the following should she do FIRST?

- (A) Follow the link and promptly update her personal details to avoid any inconvenience
- (B) Forward the email to her friends and family to ensure

they are also aware of the bank's system upgrade

- (C) Delete the email immediately without taking any action
- (D) Contact her bank through official channels to verify the authenticity of the email

Question 126. A user receives an SMS claiming to be from her bank, alerting her of unauthorized activity on her account. The message instructs the user to immediately click on a provided link and verify her account details. The user hasn't noticed any irregularities with her bank account. Which type of attack is this SMS most likely part of?

- (A) Smishing
- (B) Vishing
- (C) Bluejacking
- (D) Bluesnarfing

Question 127. An e-commerce platform reported a series of breaches over the past month. With each breach, financial and personal data of thousands of users were exfiltrated. The perpetrators subsequently sold the data on the dark web. Which type of threat actor is MOST likely behind these breaches?

- (A) Insider threat
- (B) Hacktivist
- (C) Organized crime syndicate
- (D) Nation-state

Question 128. Alex, a new intern at an IT company, wanted to access the internal company portal. Instead of typing "companyportal.com," he accidentally typed "comapnyportal.com" and ended up on a site that looked identical but asked him to download a security certificate. This

scenario best describes which type of attack?

- (A) Spear Phishing
- (B) Watering Hole Attack
- (C) Typosquatting
- (D) Man-in-the-Middle

Question 129. A major pharmaceutical company recently announced an increase in drug prices. Following the announcement, their website was taken offline by a DDoS attack, with a message posted online by a group claiming responsibility and demanding affordable healthcare for all. Which type of threat actor is MOST likely behind this attack?

- (A) Unskilled attacker
- (B) Insider threat
- (C) Hacktivist
- (D) Nation-state

Question 130. A government agency experienced a cyber incident where its communication platforms were breached. The intruders were not interested in extracting sensitive data or causing disruptions but were observed to be silently monitoring diplomatic communications for an extended period. What was the likely motivation of the attackers?

- (A) To gain financial benefits from insider trading
- (B) Espionage to understand and anticipate diplomatic moves
- (C) Disgruntlement of an internal employee
- (D) An attempt to expand their cybercriminal network

Question 131. Employees at a renowned software development firm frequently visit an industry-related forum to discuss the

latest trends and technologies. Over the past month, several employees reported malware infections shortly after accessing the forum. An investigation suggests the forum was compromised to target the company's developers specifically. Which type of attack most accurately describes this scenario?

- (A) Spear Phishing
- (B) Watering Hole
- (C) Drive-by Download
- (D) Whaling

Question 132. A cybersecurity analyst has noticed a series of sophisticated attacks against critical infrastructure systems in their country. The attacks are highly coordinated, well-funded, and appear to have specific geopolitical objectives. Which type of threat actor is MOST likely responsible for these attacks?

- (A) Organized crime syndicates
- (B) Script kiddies
- (C) Insider threat
- (D) Nation-state

Question 133. A small business detected unauthorized access to its website. The attacker used default login credentials to gain access. What level of sophistication and capability does this attack suggest about the threat actor?

- (A) Script kiddie with basic skills
- (B) Expert attacker leveraging advanced techniques
- (C) Nation-state actor with strategic objectives
- (D) Organized crime syndicate targeting high-value assets

Question 134. Tech Enterprises is planning to release a new product. As part of the product's creation, they've sourced

components from various vendors. The security team is tasked with assessing risks linked to the supply chain. Which of the following is the MOST concerning risk when sourcing components from multiple vendors?

- (A) Difficulty in tracking product warranty details from multiple vendors
- (B) Increased product assembly time due to varied vendor delivery timelines
- (C) Potential for introduction of insecure or compromised components
- (D) The need for multiple purchase orders, leading to increased paperwork

Question 135. An employee of XYZ Corp downloaded a seemingly benign PDF file from a vendor's website. After opening the PDF, the company's intrusion detection system (IDS) alerted the security team about suspicious activity originating from the employee's computer. The PDF file most likely contained which of the following threats?

- (A) Watering Hole Attack
- (B) Malicious Macro
- (C) SQL Injection
- (D) Credential Harvesting

Question 136. John, a security analyst, noticed an increase in unauthorized devices connecting to the company's wireless network. To identify the reason, he realized that the wireless access points were still using an old encryption standard. Which outdated encryption standard is likely in use that is known to be easily compromised?

- (A) WPA3

- (B) WEP
- (C) WPA2-PSK
- (D) AES

Question 137. Lucy, a security analyst, is informed that several employees have been receiving unauthorized file transfer requests via Bluetooth when they are in the company's cafeteria. Which of the following attacks is MOST likely being attempted?

- (A) Bluejacking
- (B) ARP poisoning
- (C) Bluesnarfing
- (D) Evil Twin

Question 138. Country A and Country B are engaged in an ongoing territorial dispute. Suddenly, critical infrastructure facilities in Country B, such as power plants and transportation hubs, experience systematic cyberattacks. No ransom demand is made, and the attacks lead to significant disruption. What is the most probable motivation behind these cyberattacks?

- (A) Financial gain from market disruptions
- (B) Ethical hackers testing vulnerabilities
- (C) Disruption due to philosophical disagreements with Country B's policies
- (D) Acts of cyberwarfare to weaken Country B's position

Question 139. Maria receives a text message on her phone from an unknown number, stating that she has won a gift card worth \$500 from a popular online store. The message includes a link asking her to click on it to claim her prize. Maria is unsure about the authenticity of the message. Which of the following is

the BEST course of action for Maria?

- (A) Click the link to check if the website looks genuine
- (B) Forward the message to her friends to verify if they received a similar message
- (C) Delete the message without clicking on any links
- (D) Respond to the sender asking for more details about the offer

Question 140. A retail company recently suffered a breach where attackers encrypted all point-of-sale systems, rendering them unusable. A ransom note was then received, demanding payment in cryptocurrency to decrypt the systems. What motivation is most evident behind this attack?

- (A) Protesting against the company's environmental policies
- (B) Financial gain through ransom
- (C) Espionage to understand the company's supply chain
- (D) Seeking a reputation boost by showing off technical skills

Question 141. A company detected a DDoS attack that lasted for several weeks. The attackers used a botnet of millions of infected devices and frequently rotated attack vectors to bypass mitigation efforts. This prolonged and resource-intensive attack suggests which kind of threat actor's resources and funding?

- (A) Amateur hacker with minimal resources
- (B) Cybersecurity researcher testing vulnerabilities
- (C) Nation-state actor with strategic interests
- (D) Organized crime syndicate with substantial funding

Question 142. In a routine security assessment, Claire found that a newly deployed database server within her organization is

still using its default login credentials. Which of the following is the PRIMARY security risk associated with this finding?

- (A) The database will not function optimally
- (B) The server will need frequent patches
- (C) Unauthorized individuals may easily gain access
- (D) The server will consume more bandwidth

Question 143. During a major sports event, a broadcasting company's streaming services were taken offline by a sudden surge in traffic. The attack continued for the duration of the event and then subsided. What was the most probable motivation behind this attack?

- (A) Espionage to intercept sensitive communications
- (B) To cause a service disruption during the sports event
- (C) Data exfiltration for future ransom demands
- (D) To gain unauthorized access and implant malware

Question 144. An employee receives a call from someone claiming to be from the IT department. The caller says there's an urgent update required on the employee's computer and asks for login credentials to perform the update remotely. The employee becomes suspicious because of which red flag regarding impersonation?

- (A) The caller did not use technical jargon
- (B) IT normally sends email notifications about updates
- (C) The employee was not expecting any updates
- (D) The caller's voice sounded unfamiliar

Question 145. During an e-commerce website audit, a security analyst discovers that if a user tries to purchase a product and simultaneously cancels the order, the product sometimes gets

added to the user's cart without deducting any funds. This vulnerability can potentially be exploited to obtain products for free. Which vulnerability type is the e-commerce website susceptible to?

- (A) Directory Traversal
- (B) Insecure Direct Object References (IDOR)
- (C) Race Condition
- (D) Cross-Site Request Forgery (CSRF)

Question 146. Maria, a network administrator, receives a report detailing several open service ports on critical company servers. She wants to verify the accuracy of the report. Which of the following tools would be BEST for Maria to use to validate the findings?

- (A) Password cracker
- (B) Port scanner
- (C) IDS (Intrusion Detection System)
- (D) Web application firewall

Question 147. John, a senior executive at XYZ Corp., gets a call from someone claiming to be from the bank's fraud department. The caller asks John to confirm certain transactions by providing the OTP sent to his registered mobile number. What form of social engineering attack is John likely facing?

- (A) Baiting
- (B) Quizzing
- (C) Vishing
- (D) Pharming

Question 148. Jane, a security analyst, receives a report about network slowdowns happening at specific times of the day.

After investigating, she discovers that a device is flooding the network with traffic, causing legitimate requests to be dropped. Which type of attack is this device likely performing?

- (A) Distributed Denial of Service (DDoS)
- (B) ARP poisoning
- (C) MAC flooding
- (D) DNS amplification

Question 149. A software development team in a large corporation decided to use an unauthorized cloud-based tool to host and manage their source code. The team believed it would increase their productivity, even though it was not approved by the IT department. A few weeks later, unauthorized access to their project data was detected. Which threat actor concept BEST describes the situation?

- (A) Insider threat
- (B) Hacktivist
- (C) Shadow IT
- (D) Organized crime syndicate

Question 150. A software company recently discovered a vulnerability in its popular application, which allowed unauthorized access to users' data. Before the company could release a patch, a group of hackers exploited the vulnerability but only to notify the users about it. They did not misuse any data. What is the most probable motivation behind this group's action?

- (A) Financial gain by selling the data
- (B) Political beliefs against the software company's operations

- (C) Ethical concerns about user privacy and security
- (D) Desire to disrupt the software company's services

Question 151. An environmental NGO's website was hacked and replaced with a message decrying their recent campaign against deforestation, claiming they are spreading misinformation. The website was left with a manifesto promoting responsible forestry and sustainable logging practices. Which type of threat actor is MOST likely behind this incident?

- (A) Ransomware gang
- (B) Organized crime syndicate
- (C) Hacktivist
- (D) Advanced Persistent Threat (APT)

Question 152. An IT security analyst at a multinational corporation receives an email from the "HR Department" requesting urgent verification of his personal details, including his home address and social security number. The email has the company's logo but has several spelling errors. Which type of email-based threat is this email most likely representing?

- (A) Business Email Compromise (BEC)
- (B) Email bombing
- (C) Email forwarding
- (D) Phishing

Question 153. After being fired from his position as a senior network administrator at XYZ Corp, John discovered a backdoor into the company's main server that he had previously set up. He then initiated a series of Distributed Denial of Service (DDoS) attacks over a month. What is the most

probable motivation behind John's actions?

- (A) Ethical concerns about the company's data handling
- (B) Financial gain by selling access to the backdoor
- (C) Desire to research and find vulnerabilities for personal growth
- (D) Revenge against the company for his termination

Question 154. A financial institution recently discovered that a large number of confidential customer records were being accessed and copied during off-business hours. Upon investigation, it was found that the access came from an authenticated user within the company, who had recently been passed over for a promotion. Which type of threat actor is MOST likely responsible for this security incident?

- (A) Hacktivist
- (B) Insider threat
- (C) Nation-state
- (D) Organized crime syndicate

Question 155. The finance department of a global corporation found a series of unauthorized transactions originating from an employee's workstation. Investigations revealed that the employee had been bypassing company policies to make unauthorized investments using company funds. Based on the attributes of the actor, how can this threat actor be best categorized?

- (A) External actor leveraging malware
- (B) External actor exploiting vulnerabilities
- (C) Internal actor with direct access
- (D) Internal actor with indirect access

Question 156. While conducting a security assessment, Lucy found that a specific application crashes when she inputs a string that is much longer than what the input field is designed to handle. This could potentially allow her to execute arbitrary code in the application's context. What vulnerability is Lucy likely trying to exploit?

- (A) SQL Injection
- (B) Cross-Site Scripting (XSS)
- (C) Buffer Overflow
- (D) Directory Traversal

Question 157. XYZ Corp is implementing a new vulnerability scanning solution. The security team wants a solution that does not require any software to be installed on the target machines but can still identify vulnerabilities. Which type of vulnerability scanning solution should they choose?

- (A) Host-based Intrusion Detection System (HIDS)
- (B) Agentless Vulnerability Scanner
- (C) Client-based Vulnerability Scanner
- (D) Host-based Intrusion Prevention System (HIPS)

Question 158. A healthcare institution suffered a breach where medical records of high-profile patients were extracted. The data was not sold or publicly disclosed. Instead, certain individuals were approached with their personal health information and were extorted for money. What is the primary motivation behind this cyber attack?

- (A) Political activism to expose vulnerabilities in healthcare
- (B) Personal animosity targeting the healthcare institution
- (C) Financial gain through targeted extortion
- (D) Spreading malware and expanding the botnet

Question 159. During a major international sporting event, a group of unidentified hackers simultaneously launched cyberattacks against multiple infrastructures in the host city, including transportation networks, power grids, and telecommunication systems. There was no ransom demand or any clear financial motive behind the attacks. What is the most probable motivation behind these actions?

- (A) Financial gain from selling stolen data
- (B) Ethical concerns about the environmental impact of the sporting event
- (C) Revenge against a particular athlete or team
- (D) Desire to create disruption and chaos during the event

Question 160. A medium-sized financial firm has noticed a series of unauthorized transactions moving funds from legitimate accounts to overseas locations. After investigating, it was found that a group was responsible for exploiting vulnerabilities in the firm's transaction system. Which of the following motivations is most likely driving this group's actions?

- (A) Seeking notoriety within the hacker community
- (B) Financial gain from unauthorized transactions
- (C) Demonstrating political beliefs against financial institutions
- (D) Espionage to uncover the firm's investment strategies

Question 161. An organization's e-commerce platform experienced a data breach where attackers exploited a known vulnerability. Post-incident analysis revealed that a patch was available for this vulnerability two months before the breach but was not applied. Which of the following would have been the

MOST effective measure to prevent this breach?

- (A) Implementing stronger user authentication methods
- (B) Increasing network monitoring for signs of malicious activity
- (C) Applying the available patch in a timely manner
- (D) Migrating to a different e-commerce platform

Question 162. Sophia, a network administrator, is reviewing the logs from the company's Intrusion Detection System (IDS). She notices an increased amount of outbound traffic to an unfamiliar IP address. Upon deeper analysis, she found that the traffic consists of sensitive data being transferred. What type of malicious code might be responsible for this?

- (A) Ransomware
- (B) Adware
- (C) Data Exfiltration Malware
- (D) Keylogger

Question 163. During a security assessment of an application, Ryan found that he was able to input larger-than-expected data into a field. Upon doing so, he noticed the application became unresponsive and eventually crashed. What type of vulnerability might Ryan have uncovered?

- (A) Input Validation Error
- (B) Cross-Site Scripting (XSS)
- (C) Buffer Overflow
- (D) Insecure Direct Object Reference (IDOR)

Question 164. Jake recently ran an old game on his computer that he received from a friend. Shortly after, he discovered that some of his documents were duplicated with slight

modifications, and his system's performance was deteriorating. Which kind of malware most likely caused these issues?

- (A) Adware
- (B) Trojan
- (C) Worm
- (D) Virus

Question 165. The IT department of an e-commerce company is configuring access controls for a new online product inventory system. They want the sales team to update the inventory levels and product details but don't want them to access financial data stored in the same system. Which access control principle is the IT department applying?

- (A) Least Privilege
- (B) Role-Based Access Control (RBAC)
- (C) Mandatory Access Control (MAC)
- (D) User-Based Access Control (UBAC)

Question 166. The IT team at a manufacturing company is deploying an IoT-based monitoring system for their machinery. They want to ensure that these IoT devices, if compromised, cannot adversely affect their main corporate network. What should they implement to achieve this?

- (A) Install antivirus software on all IoT devices
- (B) Regularly patch and update the IoT device firmware
- (C) Place the IoT devices on a dedicated VLAN
- (D) Enable multi-factor authentication for IoT devices

Question 167. A cloud-based collaboration tool used by a company displays a warning to a user stating, "You are logged in from two locations." However, the user has only one active

session on their workstation. What should be the primary concern for the security team?

- (A) The user might be using multiple devices
- (B) There's a potential misconfiguration in the tool's settings
- (C) The collaboration tool is facing an outage
- (D) There might be unauthorized access to the user's account

Question 168. The IT department of a software development company wants to ensure that only company-approved development tools can be executed in their development environment, preventing any unauthorized or potentially harmful software from running. What should the IT department employ to achieve this?

- (A) Implement network segmentation
- (B) Conduct regular vulnerability assessments
- (C) Install a stateful firewall
- (D) Establish an application allow list

Question 169. A large law firm has a centralized document repository where lawyers store client information, legal drafts, and other sensitive data. A new paralegal, Jenna, joins the firm and needs to be able to view client documents but should not be able to modify or delete them. Which type of permission should be granted to Jenna?

- (A) Read-Only
- (B) Full Control
- (C) Modify
- (D) Execute

Question 170. A company is developing a new web application that will be processing highly sensitive user data. They want to ensure that if the web server is compromised, attackers cannot directly access the database or other critical infrastructure. Which of the following is the BEST strategy to achieve this objective?

- (A) Use strong authentication methods for the web application
- (B) Encrypt the user data at rest and in transit
- (C) Place the web server and the database server in separate network segments
- (D) Implement real-time monitoring of the web server

Question 171. An IT technician is performing a routine security audit of a company's server room. She discovers a server with outdated firmware that hasn't been updated for two years. What potential vulnerability does the outdated firmware expose the server to?

- (A) SQL Injection
- (B) Physical tampering
- (C) Unpatched exploits
- (D) Credential stuffing

Question 172. The IT department of a large organization receives reports from employees that they are unable to access certain resources on the network. Upon investigation, the IT department discovers that the Access Control List (ACL) settings have been recently modified. Which of the following would be the PRIMARY reason to review and modify the ACL settings?

- (A) To balance the network load

- (B) To update the organization's firewall rules.
- (C) To ensure appropriate access rights to resources
- (D) To update the organization's password policy

Question 173. You are a security consultant for a company that uses a cloud-based infrastructure. During a security review, you discover that there are no boundaries defined between the company's development, testing, and production environments in the cloud. This can lead to unintended interactions and data leaks. What kind of vulnerability is this scenario illustrating?

- (A) Insecure API endpoints
- (B) Weak encryption methods
- (C) Lack of resource isolation
- (D) Insufficient backup strategies

Question 174. During a routine security audit, a company discovered an unauthorized wireless access point using the same SSID as the company's official wireless network. Additionally, this rogue access point was configured without any encryption. What type of wireless attack is this scenario most indicative of?

- (A) War Driving
- (B) Wireless Phishing
- (C) Bluejacking
- (D) Evil Twin

Question 175. A system administrator notices that an unauthorized user was able to obtain elevated privileges on a server, even though the default account settings were configured correctly. Upon investigation, it was found that the server's operating system had not been updated for several months.

What type of vulnerability was likely exploited?

- (A) Application Misconfiguration
- (B) OS Patch Management Issue
- (C) Weak Encryption Algorithm
- (D) Password Reuse Attack

Question 176. A security analyst discovers that an external IP address has been repeatedly trying every possible combination of characters to gain access to the company's VPN portal for the past two days. Which type of password attack is this MOST likely describing?

- (A) Password Spraying
- (B) Dictionary Attack
- (C) Rainbow Table Attack
- (D) Brute Force Attack

Question 177. Jane, an employee at XYZ Corp, recently noticed that her browser homepage changed unexpectedly, and she's receiving an increasing number of targeted advertisements. Additionally, there's a new toolbar in her browser that she doesn't remember installing. Based on these symptoms, which type of malware is most likely affecting Jane's computer?

- (A) Ransomware
- (B) Worm
- (C) Spyware
- (D) Botnet

Question 178. A software developer at XYZ Corp included a piece of code in the company's software that would corrupt the application's databases if his name was ever removed from the

list of contributors in the application credits. Months after he left the company, the application databases were corrupted after an update. What type of malware was responsible for this action?

- (A) Trojan
- (B) Spyware
- (C) Adware
- (D) Logic bomb

Question 179. A popular online shopping platform noticed that some product reviews contained a strange link which, when clicked, led users to a site that resembled the platform but harvested login credentials. What vulnerability in the review system might have allowed attackers to post such links?

- (A) Session Hijacking
- (B) Cross-site scripting (XSS)
- (C) Password Spraying
- (D) Credential Stuffing

Question 180. During a routine security review, a security analyst discovers multiple failed login attempts to a secure server room's electronic access control system, all within a short time span. The access logs show a sequential pattern of access codes being tried. What type of physical attack is likely being attempted?

- (A) Tailgating
- (B) Phishing
- (C) Brute force
- (D) Social engineering

Question 181. A multinational corporation communicates sensitive information between its branches using encryption. An internal audit reveals that the encryption algorithms being used are those that were deprecated several years ago. Which of the following cryptographic vulnerabilities is the organization most exposed to?

- (A) Key generation flaw
- (B) Weak algorithms susceptible to attacks
- (C) Inadequate public key infrastructure
- (D) Mismanagement of cryptographic keys

Question 182. During a routine audit of the corporate servers, the system administrator discovers that a week's worth of security logs are missing from one of the key application servers. Which of the following is the MOST likely reason for this occurrence?

- (A) The logging service experienced a malfunction
- (B) There was insufficient storage space for the logs
- (C) A malware attack aimed to erase traces of intrusion
- (D) The time zone setting was incorrectly configured

Question 183. The content filtering logs at a retail company display multiple instances of blocked access to a file download URL ending with “.exe”. The source IP address belongs to a point of sale (POS) terminal. What should be the primary concern for the security team?

- (A) The POS terminal might have outdated software
- (B) There's a possible misconfiguration in the content filtering rules
- (C) The POS terminal might be compromised and trying to

download malicious executables

(D) The company's internet speed is too slow

Question 184. Kara, a financial analyst, began to notice unusual account activity tied to her credentials. She is sure she hasn't initiated these transactions. Upon further investigation, IT discovered a program on her computer that was recording her keystrokes. What type of malware was found on Kara's computer?

(A) Ransomware

(B) Keylogger

(C) Adware

(D) Rootkit

Question 185. A finance department employee, Maya, is transferred to the HR department. The IT department is considering her access requirements. Which of the following actions aligns best with the principle of least privilege?

(A) Retain Maya's access to the finance system and grant additional access to the HR system

(B) Remove all previous access rights and provide her access solely to the HR system

(C) Grant Maya administrative rights to ease her transition between departments

(D) Limit Maya's access to read-only for both finance and HR systems for a transitional period

Question 186. During a security audit, a company realized that a malicious actor was able to situate themselves on the network path, capturing TLS handshake messages between clients and the server. The attacker's goal is to weaken the encryption by

influencing the cipher suite negotiation process. What type of network attack does this scenario depict?

- (A) ARP Poisoning
- (B) Downgrade Attack
- (C) SYN Flood
- (D) Ping of Death

Question 187. A developer has implemented a new feature on a company's website that allows users to search for products by their names. Within a few days, the IT team noticed abnormal activities where entire tables from the database were being dumped. Which vulnerability might the new feature have introduced?

- (A) Cross-Site Scripting (XSS)
- (B) Distributed Denial-of-Service (DDoS)
- (C) Structured Query Language injection (SQLi)
- (D) Cross-Site Request Forgery (CSRF)

Question 188. During a routine security assessment, Jake, a penetration tester, discovers that by modifying a configuration file located in a public directory, he can assign himself administrative privileges in the application. What type of vulnerability is Jake exploiting?

- (A) Cross-Site Scripting (XSS)
- (B) Privilege Escalation
- (C) SQL Injection
- (D) Insecure Direct Object Reference (IDOR)

Question 189. An organization's security team discovered that an attacker had gained unauthorized access to a server. Upon investigating, they found a software tool that allowed the

attacker to mask processes, files, and system data, effectively remaining hidden while maintaining privileged access. What type of malware was implanted by the attacker?

- (A) Trojan
- (B) Worm
- (C) Logic Bomb
- (D) Rootkit

Question 190. The IT team of XYZ Corp received an alert that an employee's account was used to access the company's portal from Paris at 2:00 PM and then from Tokyo at 2:30 PM. The employee is currently on a business trip to Paris. What could this alert be indicating?

- (A) The employee quickly traveled from Paris to Tokyo
- (B) The company's time zone settings are misconfigured
- (C) There's a possible VPN misconfiguration on the employee's computer
- (D) The employee's account might have been compromised

Question 191. An organization recently deployed a cloud-based database to support its new application. A few weeks later, unauthorized access to the database was detected. An investigation revealed that the database was accessible without a password. Which of the following misconfigurations is primarily responsible for the security breach?

- (A) Default configurations left unchanged
- (B) Insufficient network segmentation
- (C) Encryption not enabled at rest
- (D) Lack of intrusion detection system

Question 192. A user reports that whenever they try to visit their online banking website, they are redirected to a website that looks identical but has a slightly different URL. The fake website asks for additional personal details that the bank never requested before. Which type of DNS attack is the user likely encountering?

- (A) DNS Tunneling
- (B) DNS Fast Flux
- (C) DNS Cache Poisoning
- (D) Domain Hijacking

Question 193. Alex recently purchased a new laptop. Upon first startup, he noticed multiple pre-installed software applications, most of which he didn't recognize or find necessary. The laptop's performance was slower than expected given its hardware specifications. Which type of software is most likely causing this performance degradation?

- (A) Ransomware
- (B) Bloatware
- (C) Spyware
- (D) Adware

Question 194. The IT department of a large corporation is performing a vulnerability assessment on its virtualized infrastructure. They come across a potential threat where a user from within a VM can interact and possibly compromise the host system. What is this type of vulnerability commonly referred to as?

- (A) VM cloning
- (B) VM snapshotting

- (C) VM escape
- (D) VM migration

Question 195. A renowned technology company recently released a new line of routers. After a short period, security researchers discovered that some of these routers contain malicious chips embedded during the manufacturing process. This incident most likely represents a vulnerability related to which supply chain aspect?

- (A) Outsourced software development risks
- (B) Service provider's outdated security practices
- (C) Hardware provider's embedded compromise
- (D) Inadequate vendor background checks

Question 196. A large news website was rendered unavailable during a major news event. Network logs show an overwhelming amount of traffic from IoT devices. Which type of DDoS attack leveraged IoT devices is this indicative of?

- (A) Reflected Attack
- (B) Botnet Attack
- (C) Amplification Attack
- (D) Teardrop Attack

Question 197. A web application requires users to authenticate using a token sent to their email. Alex, a security analyst, observes that once logged in, if he presents the same token again, he is granted access without any restrictions. What type of vulnerability does this situation depict?

- (A) Cross-Site Request Forgery (CSRF)
- (B) Replay Attack

- (C) Man-in-the-Middle (MitM) Attack
- (D) Cross-Site Scripting (XSS)

Question 198. Liam, a security analyst, is investigating a potential breach. He discovers that a malicious actor sent requests to the server by altering HTTP headers to impersonate another user, thereby gaining unauthorized access. Which type of application attack is this?

- (A) Cross-Site Request Forgery (CSRF)
- (B) Cross-Site Scripting (XSS)
- (C) HTTP Header Forgery
- (D) Session Hijacking

Question 199. A company's network administrator notices that several switches in the network infrastructure are no longer receiving firmware updates from the manufacturer. These devices are no longer sold or supported. What vulnerability do these switches introduce to the network?

- (A) Physical hardware tampering
- (B) Lack of redundancy
- (C) Increased susceptibility to new threats
- (D) Wireless interference

Question 200. While reviewing web server logs, Sarah, a security analyst, notices a pattern of requests containing “..%2F..” in the URLs. She suspects this might be an attempt to exploit a vulnerability. Which type of application attack is likely being attempted?

- (A) Command Injection
- (B) Cross-Site Scripting (XSS)

- (C) Directory Traversal
- (D) Cross-Site Request Forgery (CSRF)

Question 201. A security analyst is reviewing network logs and notices that an attacker positioned in between the user and the target website is intercepting and potentially modifying the user's communications before passing them on to the intended destination. This malicious activity occurs transparently, with neither the user nor the target website being aware. What type of network attack is being described?

- (A) Replay Attack
- (B) Smurf Attack
- (C) On-path Attack
- (D) Spoofing Attack

Question 202. A financial firm outsources its payment processing to a third-party service provider. After a series of fraudulent transactions, it was discovered that the service provider was not employing the latest encryption standards when transmitting data. Which vulnerability related to supply chain does this scenario highlight?

- (A) Inadequate vendor background checks
- (B) Service provider's outdated security practices
- (C) Deficient hardware components from a supplier
- (D) Software with embedded backdoors

Question 203. Julia, a cybersecurity analyst, notices a recently installed application named "PhotoEditorPro.exe" on a corporate workstation. Upon further inspection, she identifies that this application is silently exfiltrating sensitive company data to an external IP address. Which type of malware is Julia

most likely observing?

- (A) Worm
- (B) Ransomware
- (C) Trojan
- (D) Adware

Question 204. A company's IT department notices a sharp increase in account lockouts over the past two days, especially during non-business hours. While some accounts are from various departments, a majority are from the finance team. Which of the following is the MOST plausible explanation for these lockouts?

- (A) Scheduled maintenance by the IT department
- (B) Employees are sharing passwords within the finance team
- (C) An attacker is trying to gain unauthorized access
- (D) A recent password policy change requiring more frequent changes

Question 205. Sarah, a software developer at a tech company, decided to gain root access to her company-issued mobile device to customize its features. Soon after, the IT department detected unauthorized data transmissions from her device. Which mobile vulnerability is most likely associated with her actions?

- (A) Side loading of applications
- (B) Inconsistent OS updates
- (C) Mobile device jailbreaking
- (D) Use of open Wi-Fi networks

Question 206. After a recent cyber attack on a corporation's central database, the IT department has been tasked with enhancing the security of their network infrastructure. Which of the following would be the BEST technique to ensure that different departments, like HR and Finance, cannot access each other's sensitive data?

- (A) Implement network segmentation based on departments
- (B) Upgrade the bandwidth of the entire network
- (C) Use a single strong password for all departments
- (D) Move all department data to the cloud

Question 207. During an organization's security review, the cybersecurity analyst noticed that there were multiple failed login attempts for different user accounts, each with a few commonly used passwords. What type of password attack does this scenario BEST describe?

- (A) Brute Force Attack
- (B) Dictionary Attack
- (C) Credential Stuffing
- (D) Password Spraying

Question 208. The IT team at TechnoCorp has noticed a consistent pattern over the last week where a particular server's CPU usage spikes to 100% between 2:00 AM and 4:00 AM, a time when there's typically minimal user activity. What could be the MOST probable reason for this?

- (A) The server is automatically updating its software
- (B) An employee is running a heavy computational task
- (C) The server is undergoing a DDoS attack
- (D) Malware is performing cryptomining activities

Question 209. An organization's IT department noticed a rapid increase in network traffic over the past 24 hours.

Simultaneously, many employees reported that their systems have been slow and that they received a file named "updatePatch.exe" from coworkers via email, even though the coworkers did not intentionally send any files. What type of malware is most likely responsible for this behavior?

- (A) Trojan
- (B) Ransomware
- (C) Adware
- (D) Worm

Question 210. During a routine check, an IT technician notices several files on a company server have been renamed with a ".locked" extension and there's a new file named "README_TO_RECOVER_FILES.txt" present in the root directory. Based on these indicators, which type of malicious activity is most likely in progress?

- (A) Worm propagation
- (B) Trojan horse execution
- (C) Ransomware attack
- (D) Logic bomb activation

Question 211. An organization is choosing a hash function for digital signatures. They want to ensure that it is resistant to scenarios where an attacker might produce two different messages having the same hash. Which type of attack are they trying to defend against?

- (A) Side-channel Attack
- (B) Replay Attack

- (C) Birthday Attack
- (D) Ciphertext-only Attack

Question 212. An IT security team received reports that a new, previously unknown vulnerability was being actively exploited in the wild. The software vendor has not yet provided a patch for the vulnerability. What is the most accurate term for this vulnerability?

- (A) Legacy vulnerability
- (B) Zero-day vulnerability
- (C) Patched vulnerability
- (D) Known vulnerability

Question 213. A company has recently deployed a new e-commerce application. The security team wants to ensure they can detect any unauthorized or malicious activities on the application. Which of the following would be the MOST effective way to achieve this goal?

- (A) Conduct a penetration test on the application
- (B) Install a firewall in front of the application
- (C) Implement continuous monitoring of the application's logs and activities
- (D) Provide training to users about secure browsing habits

Question 214. Ella, a security analyst, is reviewing the logs of a web application and notices that an attacker attempted to use the following input in a login form: ' OR '1'='1' --. This input was used in an effort to manipulate the application's backend database. What type of injection attack is this an example of?

- (A) XML Injection
- (B) Command Injection

- (C) SQL Injection
- (D) LDAP Injection

Question 215. A medium-sized company has just deployed a new file server for the HR department. They want to ensure that only HR employees can view and edit HR-specific documents, while the IT department should only be able to perform system maintenance tasks. What should the company implement to achieve this requirement?

- (A) Install a firewall between the HR and IT departments
- (B) Implement an Access Control List (ACL) for the file server
- (C) Enforce a strong password policy for the HR department
- (D) Enable full disk encryption on the file server

Question 216. An e-commerce website suddenly experiences a sharp increase in traffic, causing the website to become slow and occasionally inaccessible. The IT team observes that a large number of requests are originating from multiple IP addresses spread across various countries. What type of network attack is the e-commerce website likely experiencing?

- (A) Man-in-the-middle attack
- (B) DNS spoofing
- (C) Distributed denial-of-service (DDoS) attack
- (D) ARP poisoning

Question 217. A security auditor found that a website's login form returns detailed error messages like "Incorrect column name" or "Table not found." Which type of vulnerability could attackers potentially exploit using this information?

- (A) Brute Force Attack

- (B) Structured Query Language injection (SQLi)
- (C) Man-in-the-Middle Attack
- (D) Session Hijacking

Question 218. An employee at a large corporation has recently installed an app on his company-issued mobile device from a website instead of the approved app store. The app claimed to help boost productivity, but soon after, sensitive data from the mobile device was found to be transmitted to an unknown server. What mobile vulnerability was exploited?

- (A) Inadequate password policies
- (B) Open Wi-Fi connection
- (C) Mobile device side loading
- (D) Lack of mobile device encryption

Question 219. The IT department of XYZ Corp noticed that server logs are recording user login attempts during non-business hours, specifically between 2:00 AM and 3:00 AM, a time when no scheduled tasks or backups are set to run. Which of the following is the MOST plausible explanation for this unusual activity?

- (A) The company's employees are working overtime
- (B) There might be a time zone misconfiguration on the server
- (C) An unauthorized user is trying to gain access to the server
- (D) The server is automatically installing security patches

Question 220. An employee notices a stranger standing unusually close to her with an unfamiliar device while she uses her RFID badge to enter the office building. A few days later,

her colleague's badge suddenly stops working, even though it was not reported lost or damaged. What type of attack should the security team suspect?

- (A) Brute force attack on the access control system
- (B) RFID cloning
- (C) Tailgating
- (D) RFID jamming

Answers 111-220

Question 111. A medium-sized company suffered a data breach. Investigations revealed that an attacker from a rival firm had exploited a misconfigured firewall to gain unauthorized access to the company's database. Based on the attributes of the actor, how would this threat actor be best described?

- (A) Internal actor leveraging physical access
- (B) Internal actor abusing privileges
- (C) External actor using social engineering
- (D) **External actor exploiting technical vulnerabilities**

Explanation 111. Correct Answer: D. External actor exploiting technical vulnerabilities. The attacker originated from outside the victim organization (a rival firm) and exploited a technical issue (misconfigured firewall) to gain access. This categorizes them as an external actor exploiting technical vulnerabilities.

Option A is incorrect. The attacker was from a rival firm and did not utilize physical access within the victim organization. Therefore, this description doesn't match the scenario.

Option B is incorrect. The scenario doesn't mention any internal actors or abuse of privileges. Instead, it describes an external attacker from a rival firm.

Option C is incorrect. While the attacker was external, the scenario does not describe any use of social engineering tactics. Instead, the attacker exploited a technical vulnerability (misconfigured firewall).

Question 112. Sophia, the CFO of a medium-sized company, received a call from an individual claiming to be from the IT department. The caller requested her login details for a “critical system update.” Suspecting something wasn't right, Sophia hung up and contacted her IT department, which confirmed no such call was made by them. Which type of attack did Sophia most likely experience?

- (A) **Vishing**
- (B) Phishing
- (C) SQL Injection
- (D) Cross-Site Request Forgery (CSRF)

Explanation 112. Correct Answer: A. Vishing. Vishing, or voice phishing, is an attack where fraudsters use the telephone to mislead individuals into revealing personal information or login credentials.

Option B is incorrect. Phishing is typically an attempt to obtain sensitive information through deceptive emails and websites, not voice calls.

Option C is incorrect. SQL Injection is an attack type that tries to execute malicious SQL statements in a database. It is not related to voice calls.

Option D is incorrect. Cross-Site Request Forgery (CSRF) is a type of attack where the attacker tricks the victim into submitting a malicious request. This is unrelated to voice call scenarios.

Question 113. During an incident response, the IT team discovers malware that collects information about military projects. The malware sends the data to a server located in a foreign country. Which type of threat actor would MOST likely be involved in this type of cyber espionage?

- (A) Disgruntled employee
- (B) **Nation-state**
- (C) Phishing scam artist
- (D) Hacktivist

Explanation 113. Correct Answer: B. Nation-state. Malware that specifically targets information about military projects and sends data to a foreign server is indicative of cyber espionage, a tactic commonly employed by nation-states. They have the motivation to gather intelligence and potentially disrupt or gain advantages over other nations, particularly concerning military or defense-related data.

Option A is incorrect. While a disgruntled employee might have a motive to harm the company, they wouldn't typically be involved in the collection of military project information for a foreign nation.

Option C is incorrect. Phishing scam artists primarily focus on deceiving individuals into revealing personal or financial information. They typically don't have interest or resources for collecting military-specific data for foreign espionage.

Option D is incorrect. Hacktivists are typically motivated by ideological, environmental, or political causes. While they might disrupt services or leak information, targeting military projects for a foreign nation isn't a typical characteristic of their activities.

Question 114. A company's website was temporarily defaced with a humorous meme, but no sensitive data was stolen or any significant damage done. The attacker left a message bragging about their first successful hack. Which type of threat actor is MOST likely responsible for this attack?

- (A) Insider threat
- (B) Advanced Persistent Threat (APT)
- (C) **Unskilled attacker**
- (D) Nation-state

Explanation 114. Correct Answer: C. Unskilled attacker.

Unskilled attackers, often referred to as "script kiddies", typically utilize pre-made tools or scripts to carry out basic attacks. Their motivations are often more about bragging rights or minor mischief, such as defacing a website for fun or to prove they can, rather than executing a sophisticated or damaging attack.

Option A is incorrect. Insider threats are individuals within an organization that may have specific motives related to personal

grievances or financial gain. Their attacks would typically be more targeted and potentially more harmful than just defacing a website.

Option B is incorrect. Advanced Persistent Threats (APTs) are highly skilled and typically represent organized groups with specific, long-term objectives. Their attacks are sophisticated and stealthy, aiming for data theft or system compromise over an extended period.

Option D is incorrect. Nation-states are motivated by political, military, or espionage objectives. A simple website defacement, especially one with a humorous meme, does not align with their typical motivations or methods.

Question 115. A new technology firm recently launched a device that uses facial recognition for authentication. A cybersecurity researcher, without any malicious intent, demonstrated a method to bypass the facial recognition using a photograph. The researcher then approached the firm with the findings without publicizing it. What is the primary motivation behind the researcher's action?

- (A) Philosophical beliefs opposing facial recognition
- (B) Financial gain by blackmailing the firm
- (C) **Ethical considerations for consumer security**
- (D) Aiming to damage the firm's market reputation

Explanation 115. Correct Answer: C. Ethical considerations for consumer security. By responsibly disclosing the vulnerability to the firm without any malicious intent or

publicizing it, the researcher showcased ethical motivations, aiming to improve consumer security.

Option A is incorrect. The researcher did not express opposition to facial recognition technology but only highlighted a potential vulnerability.

Option B is incorrect. There is no evidence that the researcher tried to blackmail the firm. Instead, they responsibly disclosed the vulnerability.

Option D is incorrect. The researcher chose not to publicize the vulnerability, indicating they were not aiming to damage the firm's reputation but to assist in improving security.

Question 116. Mike, a network administrator, notices an unauthorized device connected directly to the company's main network switch in the server room. This device is attempting to capture network traffic. What kind of attack is this unauthorized device likely conducting?

- (A) Rogue access point
- (B) VLAN hopping
- (C) **Port mirroring**
- (D) ARP poisoning

Explanation 116. Correct Answer: C. Port mirroring. Port mirroring is a method used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port. An attacker can use this method to capture and analyze the traffic without interfering with the flow of the original packets.

Option A is incorrect. A rogue access point is a wireless access point installed on a network without the network administrator's authorization. The scenario describes a wired connection, not a wireless one.

Option B is incorrect. VLAN hopping is an attack method used to access data from different VLANs that would typically not be accessible. The scenario focuses on capturing network traffic, not crossing VLAN boundaries.

Option D is incorrect. ARP poisoning is a type of attack in which an attacker sends false ARP messages to a local network. This is not directly related to the unauthorized device connected to the switch as described.

Question 117. Alex, an employee at XYZ Corp, noticed an unfamiliar USB drive lying in the company parking lot. Out of curiosity, Alex plugged the device into his workstation. Almost immediately, his antivirus program detected malicious software trying to execute. What type of attack did Alex likely encounter?

- (A) Man-in-the-Middle Attack
- (B) Evil Twin
- (C) Spear Phishing
- (D) **USB Drop Attack**

Explanation 117. Correct Answer: D. USB Drop Attack. A USB Drop Attack involves leaving malware-infected removable devices, such as USB drives, in places where they can be found and used by unsuspecting individuals. Once the device is

plugged into a computer, it can potentially execute malicious software or scripts.

Option A is incorrect. A Man-in-the-Middle Attack involves an attacker secretly intercepting and possibly altering the communication between two parties without them noticing. It is not related to USB devices.

Option B is incorrect. Evil Twin refers to a rogue Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications. It doesn't pertain to USB devices.

Option C is incorrect. Spear Phishing is a targeted attempt to steal sensitive information through deceptive emails directed at specific individuals or companies. It is not associated with USB devices.

Question 118. A company named TechFlow is planning to produce a new line of smart home devices. They have opted to use a single supplier for a crucial component in their devices. Which of the following represents the MOST significant security risk associated with this decision?

- (A) It will be challenging to negotiate prices with just one supplier
- (B) If the supplier's delivery timeline is delayed, product launch might be postponed
- (C) **A compromise at the supplier could lead to vulnerabilities in all devices**
- (D) TechFlow will need to rely on the supplier's warranty and return policies

Explanation 118. Correct Answer: C. A compromise at the supplier could lead to vulnerabilities in all devices. Relying on a single supplier means that any security issues at that supplier's end might translate directly into vulnerabilities in every device using that component.

In a supply chain, the security of every entity is paramount. If one supplier gets compromised, and the company relies solely on that supplier for a crucial component, every product using that component might be vulnerable. This could have widespread implications for the security of the end-users and damage the company's reputation.

Option A is incorrect. Price negotiation is a business concern and not directly related to the security implications of using a single supplier.

Option B is incorrect. While delivery delays can have business implications, they don't represent a direct security risk.

Option D is incorrect. Warranty and return policies are operational considerations but aren't the primary security risks associated with relying on a single supplier.

Question 119. A high-profile executive received an email containing personal photos and a message threatening to release the images to the public unless a significant sum of money was transferred to a specific cryptocurrency address. What motivation is most evident behind this threat?

- (A) Espionage to gather competitive intelligence
- (B) Service disruption to harm the reputation of the

executive's company

(C) Blackmail to extract money by leveraging sensitive information

(D) Data exfiltration for selling on the dark web

Explanation 119. Correct Answer: C. Blackmail to extract money by leveraging sensitive information. The direct threat of releasing personal photos in exchange for money is a classic indication of blackmail. The attacker is leveraging sensitive information (personal photos) to extort money.

Option A is incorrect. There's no mention of seeking company secrets or competitive intelligence. The focus of the attacker is on personal images of the executive.

Option B is incorrect. While releasing the images might harm the executive's reputation, there's no direct intent shown to disrupt the company's services or harm its operational standing.

Option D is incorrect. The attacker is directly demanding money in exchange for not releasing the photos. This differs from data exfiltration where data might be sold or leveraged in other ways.

Question 120. Jane, an accountant in a multinational corporation, received an email from what seemed to be the company's IT department. The email had the company's logo, colors, and font and urged Jane to click on a link to reset her password due to "suspicious activity." However, upon close inspection, Jane noticed a minor spelling error in the domain name of the sender's email address. What type of attack does

this scenario describe?

- (A) Spear Phishing
- (B) Vishing
- (C) Baiting
- (D) **Brand Impersonation**

Explanation 120. Correct Answer: D. Brand Impersonation.

The attacker has mimicked the company's branding in an attempt to deceive the recipient into thinking the communication is legitimate.

Brand impersonation involves attackers mimicking or replicating the branding of a reputable company or organization in an attempt to trick users into thinking the communication is legitimate. This tactic is commonly used in phishing emails to mislead recipients into providing sensitive information or clicking on malicious links.

Option A is incorrect. Spear Phishing is targeted phishing aimed specifically at one individual or a small group. While Jane might be specifically targeted, the defining feature of this attack is the impersonation of the company's branding, making it brand impersonation.

Option B is incorrect. Vishing involves voice communication or phone calls, and the scenario describes an email-based attack.

Option C is incorrect. Baiting typically offers something enticing to lure victims. There's no offer or lure in the described scenario.

Question 121. During a routine scan, the security team at a graphic design firm discovers that an employee downloaded an image from an email and subsequently, unusual network traffic was detected originating from that employee's workstation. The image appeared normal when opened. What type of attack might have been used in this situation?

- (A) **Image Steganography Malware**
- (B) Password Brute Force
- (C) Phishing
- (D) Port Scanning

Explanation 121. Correct Answer: A. Image Steganography Malware. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. Image steganography specifically involves hiding malicious code within an image. When the image is downloaded or opened, the malicious code can be executed without the victim's knowledge.

Option B is incorrect. Password Brute Force is an attack method where an attacker attempts to guess a user's password by systematically trying every possible combination of letters, numbers, and symbols until the correct password is discovered.

Option C is incorrect. Phishing typically involves deceptive emails or messages attempting to trick recipients into divulging sensitive information. While images can be used in phishing attempts, the scenario described does not indicate an attempt to extract information from the employee.

Option D is incorrect. Port Scanning is an attempt to discover open ports on a computer, which can reveal services running on those ports. It does not involve the use of images.

Question 122. Acme Corp, a large organization, has recently entered into a contract with Zenith MSP for IT management and support. The CISO of Acme Corp is concerned about the security risks associated with this new relationship. Which of the following is the PRIMARY security concern when utilizing managed service providers (MSPs) in a supply chain?

- (A) Increased costs due to the integration of new technologies
- (B) Difficulty in ensuring consistent patch management
- (C) **Potential for unauthorized access to company resources**
- (D) Decreased IT staff morale due to outsourcing

Explanation 122. Correct Answer: C. Potential for unauthorized access to company resources. Managed Service Providers usually have elevated privileges to provide their services, potentially making them a prime target for attackers. A breach at the MSP level can lead to unauthorized access to their client's resources.

When a company engages with an MSP, that provider typically has access to critical systems, data, and network infrastructure to deliver their services. If the MSP is compromised, this can lead to a cascading effect where client systems and data are also vulnerable. It is imperative for companies to ensure their MSPs have robust security postures to prevent unauthorized access.

Option A is incorrect. While cost considerations are important in business decisions, they are not a direct security risk posed by MSPs in a supply chain.

Option B is incorrect. Though ensuring consistent patch management is a legitimate concern, the primary risk is unauthorized access through the MSP, which might have extensive privileges.

Option D is incorrect. While IT staff morale is a valid organizational concern when outsourcing, it is not the primary security risk associated with MSPs.

Question 123. Mike, an employee at a tech company, receives an instant message from a coworker named Jessica. The message contains a link and claims to showcase a hilarious video. However, Mike knows Jessica is on vacation. He suspects the message might not genuinely be from her. What type of threat is Mike most likely encountering?

- (A) Watering Hole Attack
- (B) Man-in-the-Middle Attack
- (C) **IM Spoofing**
- (D) Side-channel Attack

Explanation 123. Correct Answer: C. IM Spoofing. IM Spoofing occurs when an attacker sends messages to a system that appear to come from a trusted source, typically a known contact. By pretending to be someone the victim knows, the attacker can deceive the victim into opening a malicious link or sharing confidential information.

Option A is incorrect. A Watering Hole Attack is where the attacker guesses or observes which websites the group often uses and infects one or more of them with malware.

Option B is incorrect. A Man-in-the-Middle Attack involves the attacker secretly intercepting and relaying communication between two parties. The attacker makes independent connections with the victims and relays messages between them.

Option D is incorrect. A Side-channel Attack is based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself.

Question 124. During a political campaign, an anonymous group releases a series of articles containing fabricated data about a candidate's past, intending to influence voters' opinions. This is an example of:

- (A) Impersonation
- (B) SSmishing
- (C) **Disinformation**
- (D) Baiting

Explanation 124. Correct Answer: C. Disinformation. The spread of deliberately false information to deceive or harm, especially in sensitive areas like politics, is classified as disinformation.

Disinformation campaigns aim to deceive audiences by presenting false information as if it's true. In political scenarios,

this can have significant ramifications, affecting public opinion and the outcome of elections.

Option A is incorrect. Impersonation involves pretending to be someone else to deceive, but the scenario doesn't indicate that the anonymous group is impersonating anyone.

Option B is incorrect. Smishing is a type of phishing attack that uses SMS. It doesn't relate to spreading false information in articles.

Option D is incorrect. Baiting involves enticing victims with something they want (like free software) to steal their personal information or to spread malware. It doesn't involve the spread of false information as described in the scenario.

Question 125. Sophia received an email from her bank asking her to urgently update her personal details due to a system upgrade. The email contains a link that redirects to a website that looks similar to her bank's website. Which of the following should she do FIRST?

- (A) Follow the link and promptly update her personal details to avoid any inconvenience
- (B) Forward the email to her friends and family to ensure they are also aware of the bank's system upgrade
- (C) Delete the email immediately without taking any action
- (D) **Contact her bank through official channels to verify the authenticity of the email**

Explanation 125. Correct Answer: D. Contact her bank through official channels to verify the authenticity of the

email. Before taking action based on an unsolicited email, especially one that asks for personal information or credentials, it's essential to verify its legitimacy directly with the institution or entity it claims to represent.

Phishing attacks often use fear, urgency, or perceived authority to lure victims into providing sensitive data. The best defense against such attempts is to independently verify any unexpected or suspicious requests before taking action.

Option A is incorrect. Directly responding to a potential phishing email by providing personal details is a common mistake, making the user vulnerable to fraud and identity theft.

Option B is incorrect. Forwarding a potentially malicious email to others can further propagate the threat and possibly compromise their security as well.

Option C is incorrect. While deleting the email might prevent Sophia from falling for the phishing attempt, it's still a good practice to inform the bank about the suspicious email so they can take appropriate measures and warn other customers.

Question 126. A user receives an SMS claiming to be from her bank, alerting her of unauthorized activity on her account. The message instructs the user to immediately click on a provided link and verify her account details. The user hasn't noticed any irregularities with her bank account. Which type of attack is this SMS most likely part of?

- (A) Smishing
- (B) Vishing

- (C) Bluejacking
- (D) Bluesnarfing

Explanation 126. Correct Answer: A. Smishing. Smishing is a type of phishing attack where malicious actors use SMS to deceive individuals into providing sensitive information, typically by impersonating trusted organizations or contacts.

Option B is incorrect. Vishing refers to voice phishing, where attackers use voice calls instead of text or email to impersonate legitimate entities and scam victims.

Option C is incorrect. Bluejacking involves sending unsolicited messages to Bluetooth-enabled devices. It doesn't typically involve impersonating a legitimate entity for deceptive purposes.

Option D is incorrect. Bluesnarfing is a type of unauthorized access to or theft of information from a Bluetooth device. It doesn't involve deceptive SMS messages.

Question 127. An e-commerce platform reported a series of breaches over the past month. With each breach, financial and personal data of thousands of users were exfiltrated. The perpetrators subsequently sold the data on the dark web. Which type of threat actor is MOST likely behind these breaches?

- (A) Insider threat
- (B) Hacktivist
- (C) **Organized crime syndicate**
- (D) Nation-state

Explanation 127. Correct Answer: C. Organized crime syndicate. Organized crime syndicates are primarily motivated by financial gains. The act of exfiltrating financial and personal data from an e-commerce platform, only to sell it on the dark web, aligns with the profit-driven motives of organized crime groups.

Option A is incorrect. While insider threats can indeed pose significant risks, they are typically motivated by personal grievances, revenge, or opportunistic financial gains. The systematic breaches and subsequent sale of data on the dark web point more towards an organized group than an individual insider.

Option B is incorrect. Hacktivists primarily target organizations to further or protest a political or social cause. The described actions, focused on profiting from stolen data, are not aligned with typical hacktivist motives.

Option D is incorrect. While nation-states might engage in cyber espionage or cyber warfare for political or strategic reasons, they are not typically involved in the theft of financial data for direct monetary gain.

Question 128. Alex, a new intern at an IT company, wanted to access the internal company portal. Instead of typing “companyportal.com,” he accidentally typed “comapnyportal.com” and ended up on a site that looked identical but asked him to download a security certificate. This scenario best describes which type of attack?

(A) Spear Phishing

- (B) Watering Hole Attack
- (C) **Typosquatting**
- (D) Man-in-the-Middle

Explanation 128. Correct Answer: C. Typosquatting. The attacker relies on typographical errors made by users when inputting a URL into a web browser, then potentially tries to exploit the user in some manner on the deceptive site.

Typosquatting, also known as URL hijacking, involves attackers registering domains that are misspellings of popular websites. The intent is often to deceive users who mistype a URL, leading them to malicious websites.

Option A is incorrect. Spear Phishing targets specific individuals or companies with tailored attempts to steal information. The described scenario revolves around the exploitation of typographical errors, not a targeted email attack.

Option B is incorrect. A Watering Hole Attack involves compromising a specific website or service that the target frequently uses. It doesn't rely on typographical errors.

Option D is incorrect. A Man-in-the-Middle attack involves an attacker secretly intercepting and potentially altering communication between two parties. This is not described in the scenario.

Question 129. A major pharmaceutical company recently announced an increase in drug prices. Following the announcement, their website was taken offline by a DDoS

attack, with a message posted online by a group claiming responsibility and demanding affordable healthcare for all. Which type of threat actor is MOST likely behind this attack?

- (A) Unskilled attacker
- (B) Insider threat
- (C) **Hacktivist**
- (D) Nation-state

Explanation 129. Correct Answer: C. Hacktivist. Hacktivists are typically driven by political, social, or ideological motives. They use cyber attacks as a means to promote or protest certain issues. In this scenario, the attack on the pharmaceutical company is a form of protest against their pricing policies, making it characteristic of hacktivist behavior.

Option A is incorrect. Unskilled attackers generally conduct attacks for personal bragging rights or mischief. They are not usually driven by ideological motives like demanding affordable healthcare.

Option B is incorrect. Insider threats stem from individuals within the organization, often driven by personal grievances or financial gain. The described scenario shows a motive tied to a broader social issue, not a personal or internal motive.

Option D is incorrect. Nation-states conduct cyber operations for political, espionage, or military reasons. Protesting drug prices is not in line with their typical objectives.

Question 130. A government agency experienced a cyber incident where its communication platforms were breached. The

intruders were not interested in extracting sensitive data or causing disruptions but were observed to be silently monitoring diplomatic communications for an extended period. What was the likely motivation of the attackers?

- (A) To gain financial benefits from insider trading
- (B) **Espionage to understand and anticipate diplomatic moves**
- (C) Disgruntlement of an internal employee
- (D) An attempt to expand their cybercriminal network

Explanation 130. Correct Answer: B. Espionage to understand and anticipate diplomatic moves. Silently monitoring diplomatic communications without exfiltrating data or causing disruptions indicates a motivation to understand, anticipate, and potentially manipulate governmental or diplomatic actions. This is a classic example of espionage.

Option A is incorrect. While sensitive information might indeed be valuable for insider trading, the focus on diplomatic communications suggests a broader strategic intent rather than just financial gain.

Option C is incorrect. A disgruntled employee might engage in sabotage or data leakage, but silently monitoring diplomatic communications indicates a higher level of strategy and sophistication usually beyond personal vendettas.

Option D is incorrect. The attackers' actions were specific to monitoring diplomatic channels and did not indicate an attempt to recruit more systems or individuals into a criminal network.

Question 131. Employees at a renowned software development firm frequently visit an industry-related forum to discuss the latest trends and technologies. Over the past month, several employees reported malware infections shortly after accessing the forum. An investigation suggests the forum was compromised to target the company's developers specifically. Which type of attack most accurately describes this scenario?

- (A) Spear Phishing
- (B) **Watering Hole**
- (C) Drive-by Download
- (D) Whaling

Explanation 131. Correct Answer: B. Watering Hole. The attack focused on a particular site that employees at the targeted organization are known to visit, intending to compromise those specific individuals.

A watering hole attack involves compromising a website or online resource frequented by members of a particular group or organization. Once compromised, attackers can use the site to deploy malware to the targeted individuals.

Option A is incorrect. Spear phishing is a targeted phishing attempt, typically via email, aimed at a specific individual or organization. It does not involve compromising websites that targets frequent.

Option C is incorrect. While a drive-by download might be the method used to deliver malware once the forum was compromised, the overall strategy of targeting a specific site

known to be frequented by the victims defines it as a watering hole attack.

Option D is incorrect. Whaling is a type of phishing attack aimed at high-profile targets like CEOs or CFOs. It doesn't involve compromising websites.

Question 132. A cybersecurity analyst has noticed a series of sophisticated attacks against critical infrastructure systems in their country. The attacks are highly coordinated, well-funded, and appear to have specific geopolitical objectives. Which type of threat actor is MOST likely responsible for these attacks?

- (A) Organized crime syndicates
- (B) Script kiddies
- (C) Insider threat
- (D) **Nation-state**

Explanation 132. Correct Answer: D. Nation-state.

Sophisticated, coordinated, and well-funded attacks against national critical infrastructure with clear geopolitical objectives align most closely with the characteristics and motivations of nation-state actors. They often have vast resources and specific political or strategic motives, targeting critical infrastructures to cause significant impact or gain a strategic advantage.

Option A is incorrect. While organized crime syndicates might be well-funded and capable of launching sophisticated attacks, they are typically driven by financial motives rather than geopolitical objectives.

Option B is incorrect. Script kiddies are amateur hackers who use pre-written scripts or tools to exploit vulnerabilities. They typically lack the sophistication and resources to launch coordinated attacks against critical infrastructure.

Option C is incorrect. Insider threats come from individuals within the organization, like employees or contractors. While they can be harmful, the described scenario is more indicative of an external, nation-state actor with significant resources and geopolitical motives.

Question 133. A small business detected unauthorized access to its website. The attacker used default login credentials to gain access. What level of sophistication and capability does this attack suggest about the threat actor?

- (A) **Script kiddie with basic skills**
- (B) Expert attacker leveraging advanced techniques
- (C) Nation-state actor with strategic objectives
- (D) Organized crime syndicate targeting high-value assets

Explanation 133. Correct Answer: A. Script kiddie with basic skills. Using default login credentials for unauthorized access typically indicates a low level of sophistication, as this method is basic and requires little to no technical skill. Such attackers, often termed “script kiddies,” usually exploit known vulnerabilities with pre-existing tools or scripts without fully understanding them.

Option B is incorrect. An expert attacker would likely utilize more advanced techniques and not rely solely on default credentials.

Option C is incorrect. While nation-state actors have the capability for sophisticated attacks, the use of default login credentials as the primary method of unauthorized access doesn't align with the complex methodologies usually employed by such actors.

Option D is incorrect. Organized crime syndicates, especially those targeting high-value assets, would employ more sophisticated techniques than merely using default login credentials.

Question 134. Tech Enterprises is planning to release a new product. As part of the product's creation, they've sourced components from various vendors. The security team is tasked with assessing risks linked to the supply chain. Which of the following is the MOST concerning risk when sourcing components from multiple vendors?

- (A) Difficulty in tracking product warranty details from multiple vendors
- (B) Increased product assembly time due to varied vendor delivery timelines
- (C) **Potential for introduction of insecure or compromised components**
- (D) The need for multiple purchase orders, leading to increased paperwork

Explanation 134. Correct Answer: C. Potential for introduction of insecure or compromised components. When components are sourced from multiple vendors, there is a heightened risk that one or more components might have

vulnerabilities or could be compromised, thus impacting the security of the overall product.

The integrity and security of components are vital in product development, especially when those components are part of the supply chain from various vendors. If one vendor has lax security measures or gets compromised, the components they supply can introduce vulnerabilities into the finished product, affecting its overall security posture and potentially leading to data breaches or other cyber threats.

Option A is incorrect. While tracking warranties is an operational concern, it doesn't pose a direct security risk when sourcing components from multiple vendors.

Option B is incorrect. Product assembly time and vendor delivery timelines are logistical and operational concerns, not primary security risks associated with supply chain vendors.

Option D is incorrect. Managing multiple purchase orders is a business process challenge, not a primary security concern.

Question 135. An employee of XYZ Corp downloaded a seemingly benign PDF file from a vendor's website. After opening the PDF, the company's intrusion detection system (IDS) alerted the security team about suspicious activity originating from the employee's computer. The PDF file most likely contained which of the following threats?

- (A) Watering Hole Attack
- (B) **Malicious Macro**

- (C) SQL Injection
- (D) Credential Harvesting

Explanation 135. Correct Answer: B. Malicious Macro.

Many document types, including PDFs, can contain macros. A malicious macro can execute unwanted actions, such as downloading and installing malware, when the document is opened.

Option A is incorrect. A Watering Hole Attack is when an attacker guesses or observes which websites an organization often uses and infects them with malware, with the intent of compromising members of that organization. The scenario does not provide evidence pointing to this kind of attack.

Option C is incorrect. SQL Injection is a type of attack that aims to execute malicious SQL statements in a database. This type of attack is unrelated to opening a PDF file.

Option D is incorrect. A Drive-By Download involves automatically downloading software, often malicious, without user knowledge or consent, typically when a user visits a compromised website. The scenario specifically discusses a downloaded and then manually opened PDF.

Question 136. John, a security analyst, noticed an increase in unauthorized devices connecting to the company's wireless network. To identify the reason, he realized that the wireless access points were still using an old encryption standard. Which outdated encryption standard is likely in use that is known to be easily compromised?

- (A) WPA3
- (B) WEP
- (C) WPA2-PSK
- (D) AES

Explanation 136. Correct Answer: B. WEP. Wired Equivalent Privacy (WEP) is an old and outdated encryption protocol for wireless networks. It has several known vulnerabilities and is considered insecure, making it easier for attackers to compromise.

Option A is incorrect. WPA3 is a newer and more secure encryption protocol for wireless networks and is considered a significant improvement over previous standards.

Option C is incorrect. WPA2-PSK (Wi-Fi Protected Access 2 with Pre-Shared Key) is more secure than WEP. While it can still be targeted, it is not as easily compromised as WEP.

Option D is incorrect. AES (Advanced Encryption Standard) is an encryption standard and not a wireless encryption protocol. It is often used within WPA2 and WPA3 for securing wireless data.

Question 137. Lucy, a security analyst, is informed that several employees have been receiving unauthorized file transfer requests via Bluetooth when they are in the company's cafeteria. Which of the following attacks is MOST likely being attempted?

- (A) Bluejacking
- (B) ARP poisoning

- (C) Bluesnarfing
- (D) Evil Twin

Explanation 137. Correct Answer: A. Bluejacking.

Bluejacking is the sending of unsolicited messages or files over Bluetooth to Bluetooth-enabled devices such as mobile phones, laptops, or PDAs. It is often used as a prank or to advertise to nearby people.

Bluejacking does not give attackers control over the victim's device, but it can be used to send unwanted messages or files, which aligns with the scenario described.

Option B is incorrect. ARP poisoning is a type of attack in which an attacker sends falsified ARP (Address Resolution Protocol) messages over a local area network. It's unrelated to Bluetooth communications.

Option C is incorrect. Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection. Bluesnarfing goes beyond just sending unsolicited messages; it seeks to access personal data.

Option D is incorrect. An Evil Twin attack involves creating a rogue Wi-Fi hotspot to masquerade as a legitimate one, to intercept or manipulate data traffic. It does not directly involve Bluetooth connections.

Question 138. Country A and Country B are engaged in an ongoing territorial dispute. Suddenly, critical infrastructure facilities in Country B, such as power plants and transportation

hubs, experience systematic cyberattacks. No ransom demand is made, and the attacks lead to significant disruption. What is the most probable motivation behind these cyberattacks?

- (A) Financial gain from market disruptions
- (B) Ethical hackers testing vulnerabilities
- (C) Disruption due to philosophical disagreements with Country B's policies
- (D) **Acts of cyberwarfare to weaken Country B's position**

Explanation 138. Correct Answer: D. Acts of cyberwarfare to weaken Country B's position. Given the context of the territorial dispute and the specific targeting of critical infrastructures without any ransom demand, it's highly likely that these attacks were intended as acts of cyberwarfare by Country A or its sympathizers to exert pressure on Country B.

Option A is incorrect. While market disruptions can be exploited for financial gains, the context of a territorial dispute and the nature of the attacks suggest a motive tied to geopolitical strategy rather than financial advantage.

Option B is incorrect. Ethical hackers typically identify and report vulnerabilities rather than exploit them to cause widespread disruption.

Option C is incorrect. The attacks were too specific and large-scale to be the work of individuals or groups motivated solely by philosophical disagreements.

Question 139. Maria receives a text message on her phone from an unknown number, stating that she has won a gift card worth

\$500 from a popular online store. The message includes a link asking her to click on it to claim her prize. Maria is unsure about the authenticity of the message. Which of the following is the BEST course of action for Maria?

- (A) Click the link to check if the website looks genuine
- (B) Forward the message to her friends to verify if they received a similar message
- (C) **Delete the message without clicking on any links**
- (D) Respond to the sender asking for more details about the offer

Explanation 139. Correct Answer: C. Delete the message without clicking on any links. Messages from unknown sources, especially those that sound too good to be true, often signal a potential security threat. It's safest to delete such messages without interacting with any links.

Smishing is a type of phishing attack wherein attackers use SMS to deceive users into divulging personal information, visiting a malicious website, or downloading malware onto their smartphones. Users should always be cautious of unsolicited messages from unknown numbers.

Option A is incorrect. Clicking the link, even out of curiosity, can lead to a malicious website or download malware onto Maria's device.

Option B is incorrect. While forwarding the message to friends might give her insight into its authenticity, it could also expose her friends to potential threats if the message is malicious.

Option D is incorrect. Responding to the sender could give them more information about Maria or confirm that her number is active, leading to further targeted attacks.

Question 140. A retail company recently suffered a breach where attackers encrypted all point-of-sale systems, rendering them unusable. A ransom note was then received, demanding payment in cryptocurrency to decrypt the systems. What motivation is most evident behind this attack?

- (A) Protesting against the company's environmental policies
- (B) **Financial gain through ransom**
- (C) Espionage to understand the company's supply chain
- (D) Seeking a reputation boost by showing off technical skills

Explanation 140. Correct Answer: B. Financial gain through ransom. The attackers encrypted critical systems and then demanded a ransom to decrypt them. The primary motive in such ransomware attacks is to achieve financial gain by compelling the victim to pay to regain access to their systems.

Option A is incorrect. There's no mention or indication that the attackers were motivated by the company's environmental or any other policies.

Option C is incorrect. There's no evidence suggesting the attackers were interested in the company's supply chain or any other internal information. Their focus was on encryption and ransom.

Option D is incorrect. While demonstrating technical skills might be a byproduct of the attack, the direct demand for payment indicates that financial gain, not notoriety, is the primary motive.

Question 141. A company detected a DDoS attack that lasted for several weeks. The attackers used a botnet of millions of infected devices and frequently rotated attack vectors to bypass mitigation efforts. This prolonged and resource-intensive attack suggests which kind of threat actor's resources and funding?

- (A) Amateur hacker with minimal resources
- (B) Cybersecurity researcher testing vulnerabilities
- (C) Nation-state actor with strategic interests
- (D) **Organized crime syndicate with substantial funding**

Explanation 141. Correct Answer: D. Organized crime syndicate with substantial funding. The scale and duration of the DDoS attack, combined with the use of a massive botnet and frequent rotation of attack vectors, point to a threat actor with significant resources. While nation-states could conduct such attacks, DDoS campaigns are also a hallmark of well-funded organized crime syndicates, especially when financial or strategic extortion could be a motive.

Option A is incorrect. An amateur hacker with minimal resources would not have the capability to sustain a large-scale DDoS attack using a botnet of millions of devices over several weeks.

Option B is incorrect. Cybersecurity researchers typically do not engage in malicious activities, and launching a prolonged DDoS attack would be unethical and illegal.

Option C is incorrect. While a nation-state actor might have the resources to launch such an attack, DDoS attacks, especially those of extortion nature, are more commonly associated with organized crime syndicates.

Question 142. In a routine security assessment, Claire found that a newly deployed database server within her organization is still using its default login credentials. Which of the following is the PRIMARY security risk associated with this finding?

- (A) The database will not function optimally
- (B) The server will need frequent patches
- (C) **Unauthorized individuals may easily gain access**
- (D) The server will consume more bandwidth

Explanation 142. Correct Answer: C. Unauthorized individuals may easily gain access. Default credentials are often publicly known, and if they are not changed, malicious actors can easily use them to gain unauthorized access to systems.

Default credentials, which may include usernames and passwords set by manufacturers for initial setup, are widely known and can be easily searched online. If not changed after deployment, they pose a significant security risk as they allow anyone with this knowledge to gain access to the system.

Option A is incorrect. The use of default credentials doesn't directly impact the optimal functioning of the database.

Option B is incorrect. The use of default credentials doesn't mean that the server will need frequent patches. However, patch management is a separate aspect of maintaining server security.

Option D is incorrect. The use of default credentials doesn't directly cause the server to consume more bandwidth.

Question 143. During a major sports event, a broadcasting company's streaming services were taken offline by a sudden surge in traffic. The attack continued for the duration of the event and then subsided. What was the most probable motivation behind this attack?

- (A) Espionage to intercept sensitive communications
- (B) **To cause a service disruption during the sports event**
- (C) Data exfiltration for future ransom demands
- (D) To gain unauthorized access and implant malware

Explanation 143. Correct Answer: B. To cause a service disruption during the sports event. The surge in traffic specifically timed with the sports event and its subsequent subsiding after the event indicates a targeted intention to disrupt the service during the sports event.

Option A is incorrect. There is no indication in the scenario that the attacker was interested in intercepting communications, especially since the target was a broadcasting company and not a diplomatic or governmental agency.

Option C is incorrect. The scenario does not mention any exfiltration of data or follow-up ransom demands. The focus of the attacker was on disrupting the streaming service.

Option D is incorrect. Although taking services offline can sometimes be a cover for more malicious activities, there's no evidence in this scenario to suggest that malware was implanted or unauthorized access was achieved.

Question 144. An employee receives a call from someone claiming to be from the IT department. The caller says there's an urgent update required on the employee's computer and asks for login credentials to perform the update remotely. The employee becomes suspicious because of which red flag regarding impersonation?

- (A) The caller did not use technical jargon
- (B) **IT normally sends email notifications about updates**
- (C) The employee was not expecting any updates
- (D) The caller's voice sounded unfamiliar

Explanation 144. Correct Answer: B. IT normally sends email notifications about updates. If the organization's standard procedure is to send email notifications about updates, an unsolicited call asking for credentials would be a clear red flag.

Impersonation is a common tactic used in social engineering attacks where the attacker pretends to be someone the victim trusts. Recognizing deviations from standard procedures can help identify impersonation attempts.

Option A is incorrect. The use or lack of technical jargon isn't a reliable indicator of impersonation. Some genuine IT personnel might avoid jargon to make things clearer for non-tech-savvy employees.

Option C is incorrect. While unexpected updates can be suspicious, they aren't necessarily indicative of impersonation on their own. Legitimate unexpected updates can occur.

Option D is incorrect. An unfamiliar voice isn't a reliable indicator since large organizations might have many IT personnel that an employee hasn't interacted with.

Question 145. During an e-commerce website audit, a security analyst discovers that if a user tries to purchase a product and simultaneously cancels the order, the product sometimes gets added to the user's cart without deducting any funds. This vulnerability can potentially be exploited to obtain products for free. Which vulnerability type is the e-commerce website susceptible to?

- (A) Directory Traversal
- (B) Insecure Direct Object References (IDOR)
- (C) **Race Condition**
- (D) Cross-Site Request Forgery (CSRF)

Explanation 145. Correct Answer: C. Race Condition. When an application's unintended behavior is due to the timing of concurrent events or operations, it indicates a race condition. Here, the simultaneous purchase and cancellation result in a faulty outcome.

A race condition occurs when an application's behavior is dependent on the order or timing of uncontrollable events. If two operations, which aren't meant to happen simultaneously, occur at the same time, it can lead to unpredictable and unintended outcomes, like the described scenario where a product is added without payment due to the concurrency of purchase and cancellation.

Option A is incorrect. Directory Traversal vulnerabilities allow attackers to access files and directories that are stored outside the intended folder. This doesn't align with the described scenario.

Option B is incorrect. Insecure Direct Object References (IDOR) vulnerabilities occur when an attacker can access resources they're not authorized for by manipulating input, such as URL or form parameters. It's unrelated to the timing or concurrency of actions.

Option D is incorrect. Cross-Site Request Forgery (CSRF) tricks the victim into submitting a malicious request. It's about unauthorized actions rather than issues arising from the timing of legitimate ones.

Question 146. Maria, a network administrator, receives a report detailing several open service ports on critical company servers. She wants to verify the accuracy of the report. Which of the following tools would be BEST for Maria to use to validate the findings?

- (A) Password cracker
- (B) Port scanner

- (C) IDS (Intrusion Detection System)
- (D) Web application firewall

Explanation 146. Correct Answer: B. Port scanner. A port scanner, such as Nmap, sends packets to specific ports on a network and then listens for responses. This allows the scanner to determine which ports are open and potentially identify the services running on those ports.

Option A is incorrect. Password crackers are used to identify weak or easily guessable passwords. They don't validate open service ports.

Option C is incorrect. An IDS monitors network traffic for suspicious activity. While it can identify potential attacks, it doesn't directly verify open service ports.

Option D is incorrect. A web application firewall (WAF) protects web applications by monitoring, filtering, and blocking potentially harmful HTTP traffic. It doesn't serve the purpose of validating open service ports.

Question 147. John, a senior executive at XYZ Corp., gets a call from someone claiming to be from the bank's fraud department. The caller asks John to confirm certain transactions by providing the OTP sent to his registered mobile number. What form of social engineering attack is John likely facing?

- (A) Baiting
- (B) Quizzing
- (C) **Vishing**
- (D) Pharming

Explanation 147. Correct Answer: C. Vishing. Vishing, short for voice phishing, is the act of using the telephone to scam the user into surrendering private information that will be used for identity theft.

Vishing attacks capitalize on trust, using voice calls to manipulate victims into divulging sensitive information. Attackers often pose as legitimate entities or departments, like a bank's fraud department, to make their scam appear genuine.

Option A is incorrect. Baiting involves luring a victim into downloading malicious software under the guise of a free or beneficial download.

Option B is incorrect. Quizzing isn't a recognized type of social engineering attack.

Option D is incorrect. Pharming involves redirecting a website's traffic to a bogus site, often to capture login credentials.

Question 148. Jane, a security analyst, receives a report about network slowdowns happening at specific times of the day. After investigating, she discovers that a device is flooding the network with traffic, causing legitimate requests to be dropped. Which type of attack is this device likely performing?

- (A) Distributed Denial of Service (DDoS)
- (B) ARP poisoning
- (C) **MAC flooding**
- (D) DNS amplification

Explanation 148. Correct Answer: C. MAC flooding. MAC flooding is an attack that aims to flood the switch's MAC table with fake MAC addresses until the table overflows. Once it overflows, the switch acts as a hub broadcasting packets to all machines in the network. This can cause significant slowdowns and disruptions.

Option A is incorrect. A Distributed Denial of Service (DDoS) attack uses multiple compromised devices to flood a target with traffic, usually to overwhelm it and take it offline. The scenario describes an internal network slowdown, not an external attack on services.

Option B is incorrect. ARP poisoning is an attack where false ARP messages are sent over a local area network. It's used to link an attacker's MAC address with the IP address of another host. While it can cause disruptions, the primary intent is not to flood the network.

Option D is incorrect. DNS amplification is a type of DDoS attack where an attacker uses publically-accessible DNS servers to flood a target system with DNS response traffic. This does not fit the internal network flooding described in the scenario.

Question 149. A software development team in a large corporation decided to use an unauthorized cloud-based tool to host and manage their source code. The team believed it would increase their productivity, even though it was not approved by the IT department. A few weeks later, unauthorized access to their project data was detected. Which threat actor concept BEST describes the situation?

- (A) Insider threat
- (B) Hacktivist
- (C) **Shadow IT**
- (D) Organized crime syndicate

Explanation 149. Correct Answer: C. Shadow IT. Shadow IT refers to any IT systems or solutions used within an organization without organizational approval or oversight. This can introduce vulnerabilities, as the unauthorized systems might not meet the security standards set by the organization's IT department. In this scenario, the software development team's unauthorized use of a cloud tool exemplifies Shadow IT.

Option A is incorrect. While the software development team acted without approval, their intention was to increase productivity, not to harm the organization. Therefore, this situation does not fit the typical definition of an "insider threat," which usually has malicious intent.

Option B is incorrect. Hacktivists are motivated by political or social causes. There's no evidence in the scenario to suggest that political or social motivations were behind the team's decision.

Option D is incorrect. While the data was accessed without authorization, there's no evidence to suggest that this was the work of an organized crime syndicate. The main issue at hand is the unauthorized use of IT resources, which is a hallmark of Shadow IT.

Question 150. A software company recently discovered a vulnerability in its popular application, which allowed unauthorized access to users' data. Before the company could release a patch, a group of hackers exploited the vulnerability but only to notify the users about it. They did not misuse any data. What is the most probable motivation behind this group's action?

- (A) Financial gain by selling the data
- (B) Political beliefs against the software company's operations
- (C) **Ethical concerns about user privacy and security**
- (D) Desire to disrupt the software company's services

Explanation 150. Correct Answer: C. Ethical concerns about user privacy and security. The hackers did not misuse the data but instead chose to inform the users about the vulnerability, suggesting their motivation was based on ethical considerations to ensure users are aware of potential threats to their privacy.

Option A is incorrect. The hackers did not sell or misuse the data, which means financial gain wasn't their primary objective.

Option B is incorrect. There's no indication that the hackers' actions were driven by political beliefs against the software company.

Option D is incorrect. While the hackers did exploit a vulnerability, they did not aim to disrupt the company's services but to inform users about the vulnerability.

Question 151. An environmental NGO's website was hacked and replaced with a message decrying their recent campaign against deforestation, claiming they are spreading misinformation. The website was left with a manifesto promoting responsible forestry and sustainable logging practices. Which type of threat actor is MOST likely behind this incident?

- (A) Ransomware gang
- (B) Organized crime syndicate
- (C) **Hacktivist**
- (D) Advanced Persistent Threat (APT)

Explanation 151. Correct Answer: C. Hacktivist. The attack seems to be motivated by ideological differences regarding deforestation and sustainable logging. Hacktivists typically conduct cyber actions to make political or social statements. The replacement of the NGO's website with a manifesto supports the idea that this is an ideologically motivated attack, typical of hacktivists.

Option A is incorrect. Ransomware gangs primarily focus on encrypting data and demanding payment for its release. There is no mention of a ransom or encrypted data in the described scenario.

Option B is incorrect. Organized crime syndicates are usually motivated by financial gains. The attack on the NGO's website seems to be ideologically driven, not profit-driven.

Option D is incorrect. Advanced Persistent Threats (APTs) are highly organized, often state-sponsored groups that conduct

prolonged cyber-espionage campaigns. Their motivations are typically strategic, political, or espionage-driven. The described attack doesn't fit the profile of an APT operation.

Question 152. An IT security analyst at a multinational corporation receives an email from the “HR Department” requesting urgent verification of his personal details, including his home address and social security number. The email has the company's logo but has several spelling errors. Which type of email-based threat is this email most likely representing?

- (A) Business Email Compromise (BEC)
- (B) Email bombing
- (C) Email forwarding
- (D) **Phishing**

Explanation 152. Correct Answer: D. Phishing. Phishing emails aim to deceive recipients into sharing personal or sensitive data by impersonating a trusted source. The email's dubious quality, such as spelling errors, combined with the request for personal details, is indicative of a typical phishing attempt.

Option A is incorrect. While BEC is a type of targeted scam using email, it usually involves impersonating executives or high-ranking officials within an organization to initiate unauthorized fund transfers. The described scenario does not align with that.

Option B is incorrect. Email bombing involves sending large volumes of emails to a single recipient, typically to overwhelm

the system or hide other malicious activities. This scenario does not describe such an attack.

Option C is incorrect. Email forwarding refers to the automated redirection of email from one address to another. It is not a direct threat in itself but can be misused. The described scenario does not align with that.

Question 153. After being fired from his position as a senior network administrator at XYZ Corp, John discovered a backdoor into the company's main server that he had previously set up. He then initiated a series of Distributed Denial of Service (DDoS) attacks over a month. What is the most probable motivation behind John's actions?

- (A) Ethical concerns about the company's data handling
- (B) Financial gain by selling access to the backdoor
- (C) Desire to research and find vulnerabilities for personal growth
- (D) **Revenge against the company for his termination**

Explanation 153. Correct Answer: D. Revenge against the company for his termination. Given that John acted after being fired and initiated disruptive attacks, it's evident that his actions were motivated by a desire for revenge against his former employer.

Option A is incorrect. There's no indication in the scenario that John had ethical concerns regarding the company's data practices.

Option B is incorrect. The scenario doesn't mention John selling access to the backdoor, only that he initiated DDoS attacks.

Option C is incorrect. John's actions after termination seem malicious rather than a pursuit of knowledge or research.

Question 154. A financial institution recently discovered that a large number of confidential customer records were being accessed and copied during off-business hours. Upon investigation, it was found that the access came from an authenticated user within the company, who had recently been passed over for a promotion. Which type of threat actor is MOST likely responsible for this security incident?

- (A) Hacktivist
- (B) **Insider threat**
- (C) Nation-state
- (D) Organized crime syndicate

Explanation 154. Correct Answer: B. Insider threat. The evidence suggests the activities were conducted by an authenticated user within the organization, who might have a motive (having been passed over for a promotion). Insider threats are risks from individuals within the organization such as employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems.

Option A is incorrect. Hacktivists are typically motivated by political or social causes and will target organizations to promote or protest a specific issue. They are not usually

motivated by personal grievances like being passed over for promotions.

Option C is incorrect. Nation-states are driven by political, espionage, or military objectives. Accessing customer records of a financial institution for personal reasons doesn't align with their typical motivations.

Option D is incorrect. While organized crime syndicates might have an interest in customer records for financial gains, the inside access and the motive related to a missed promotion strongly suggest an insider threat.

Question 155. The finance department of a global corporation found a series of unauthorized transactions originating from an employee's workstation. Investigations revealed that the employee had been bypassing company policies to make unauthorized investments using company funds. Based on the attributes of the actor, how can this threat actor be best categorized?

- (A) External actor leveraging malware
- (B) External actor exploiting vulnerabilities
- (C) **Internal actor with direct access**
- (D) Internal actor with indirect access

Explanation 155. Correct Answer: C. Internal actor with direct access. The threat originated from an employee's workstation within the organization, making it an internal threat. Since the employee used their own workstation and credentials to make unauthorized transactions, they had direct access, categorizing them as an internal actor with direct access.

Option A is incorrect. There's no mention of malware being used in this scenario, and the unauthorized transactions came from an employee's workstation, indicating an internal rather than external threat.

Option B is incorrect. The scenario doesn't describe an external actor exploiting vulnerabilities. Instead, it describes an employee making unauthorized transactions from within the organization.

Option D is incorrect. The employee in this scenario had direct access to the company's resources, as they used their own workstation and credentials. Thus, they aren't categorized as having indirect access.

Question 156. While conducting a security assessment, Lucy found that a specific application crashes when she inputs a string that is much longer than what the input field is designed to handle. This could potentially allow her to execute arbitrary code in the application's context. What vulnerability is Lucy likely trying to exploit?

- (A) SQL Injection
- (B) Cross-Site Scripting (XSS)
- (C) **Buffer Overflow**
- (D) Directory Traversal

Explanation 156. Correct Answer: C. Buffer Overflow.

Buffer overflow vulnerabilities occur when data written to a buffer exceeds that buffer's boundaries, potentially overwriting adjacent memory locations. If exploited successfully, it can lead to arbitrary code execution.

Buffer overflow is a condition where an application writes more data to a buffer than it can hold, causing the excess data to overflow into adjacent memory spaces. When this happens, attackers can overwrite specific parts of the memory, which may lead to arbitrary code execution, application crashes, or data corruption.

Option A is incorrect. SQL Injection involves injecting malicious SQL statements into an entry field for execution, aiming to manipulate a database. It doesn't relate to buffer boundaries or memory overflows.

Option B is incorrect. Cross-Site Scripting (XSS) allows attackers to inject malicious scripts into web pages viewed by other users. While this is an input validation flaw like a buffer overflow, XSS specifically targets script execution within web browsers and does not involve overflowing buffer boundaries.

Option D is incorrect. Directory Traversal attacks aim to access files and directories stored outside the web root folder. They don't involve overflowing buffer boundaries or memory overflows.

Question 157. XYZ Corp is implementing a new vulnerability scanning solution. The security team wants a solution that does not require any software to be installed on the target machines but can still identify vulnerabilities. Which type of vulnerability scanning solution should they choose?

- (A) Host-based Intrusion Detection System (HIDS)
- (B) **Agentless Vulnerability Scanner**

- (C) Client-based Vulnerability Scanner
- (D) Host-based Intrusion Prevention System (HIPS)

Explanation 157. Correct Answer: B. Agentless

Vulnerability Scanner. An agentless vulnerability scanner does not require any software (agent) to be installed on the target systems. Instead, it remotely scans the systems and identifies vulnerabilities by checking against a database of known vulnerabilities.

Option A is incorrect. Host-based Intrusion Detection System (HIDS) monitors the internal workings of a computing system, not for vulnerabilities but for signs of unauthorized or malicious activity.

Option C is incorrect. Client-based Vulnerability Scanner requires an agent or software component to be installed on the target system to perform the vulnerability assessment.

Option D is incorrect. Host-based Intrusion Prevention System (HIPS) is designed to detect and prevent malicious activity on a particular device, not to scan for vulnerabilities.

Question 158. A healthcare institution suffered a breach where medical records of high-profile patients were extracted. The data was not sold or publicly disclosed. Instead, certain individuals were approached with their personal health information and were extorted for money. What is the primary motivation behind this cyber attack?

- (A) Political activism to expose vulnerabilities in healthcare
- (B) Personal animosity targeting the healthcare institution

- (C) **Financial gain through targeted extortion**
- (D) Spreading malware and expanding the botnet

Explanation 158. Correct Answer: C. Financial gain through targeted extortion. Approaching specific individuals with their personal health data for the purpose of extortion indicates a clear motivation of financial gain.

Option A is incorrect. While political activists might expose vulnerabilities in sectors like healthcare, they generally do so to raise awareness rather than for personal financial gain.

Option B is incorrect. There's no evidence from the given scenario to suggest that the attack was fueled by personal animosity towards the institution.

Option D is incorrect. The attackers' actions did not revolve around spreading malware or increasing a botnet's size but rather focused on individual extortion based on exfiltrated data.

Question 159. During a major international sporting event, a group of unidentified hackers simultaneously launched cyberattacks against multiple infrastructures in the host city, including transportation networks, power grids, and telecommunication systems. There was no ransom demand or any clear financial motive behind the attacks. What is the most probable motivation behind these actions?

- (A) Financial gain from selling stolen data
- (B) Ethical concerns about the environmental impact of the sporting event
- (C) Revenge against a particular athlete or team

(D) Desire to create disruption and chaos during the event

Explanation 159. Correct Answer: D. Desire to create disruption and chaos during the event. Given the wide array of targets and the timing of the attacks during a major event without a clear financial motive, it's evident that the main goal of the hackers was to create widespread disruption and chaos.

Option A is incorrect. There's no indication in the scenario that data was stolen or sold, and no clear financial motive was presented.

Option B is incorrect. While ethical concerns might be a possible reason for some attacks, the scale and targets of these attacks suggest a broader motive of causing disruption.

Option C is incorrect. The scenario doesn't specify any particular focus on an athlete or team; the attacks were widespread, impacting the entire event.

Question 160. A medium-sized financial firm has noticed a series of unauthorized transactions moving funds from legitimate accounts to overseas locations. After investigating, it was found that a group was responsible for exploiting vulnerabilities in the firm's transaction system. Which of the following motivations is most likely driving this group's actions?

- (A) Seeking notoriety within the hacker community**
- (B) Financial gain from unauthorized transactions**
- (C) Demonstrating political beliefs against financial**

institutions

(D) Espionage to uncover the firm's investment strategies

Explanation 160. Correct Answer: B. Financial gain from unauthorized transactions. The unauthorized transactions moving funds to overseas locations indicate a direct attempt to illicitly acquire funds, pointing towards a motivation of financial gain.

Option A is incorrect. There's no evidence to suggest the group's actions are driven by a desire for recognition or notoriety. The focus is on moving funds.

Option C is incorrect. While some groups might target financial institutions to make a political statement, the unauthorized transactions to overseas accounts suggest a financial motive, not a political one.

Option D is incorrect. There's no indication the group is interested in the firm's investment strategies. The activity is focused on moving money, not gathering intelligence.

Question 161. An organization's e-commerce platform experienced a data breach where attackers exploited a known vulnerability. Post-incident analysis revealed that a patch was available for this vulnerability two months before the breach but was not applied. Which of the following would have been the MOST effective measure to prevent this breach?

(A) Implementing stronger user authentication methods

(B) Increasing network monitoring for signs of malicious activity

- (C) Applying the available patch in a timely manner
- (D) Migrating to a different e-commerce platform

Explanation 161. Correct Answer: C. Applying the available patch in a timely manner. Patches are developed by software vendors to address known vulnerabilities in their software. Timely application of these patches is crucial to ensuring that systems are protected against known threats. In this scenario, applying the available patch would have directly addressed the vulnerability that was exploited.

Option A is incorrect. While implementing stronger user authentication methods can enhance security, it wouldn't directly mitigate a vulnerability in the software that could be exploited without authentication.

Option B is incorrect. Increasing network monitoring can help detect malicious activity, but it doesn't prevent the exploitation of a known software vulnerability.

Option D is incorrect. Migrating to a different platform is a drastic measure that might introduce new vulnerabilities and would not ensure security unless accompanied by good patch management practices.

Question 162. Sophia, a network administrator, is reviewing the logs from the company's Intrusion Detection System (IDS). She notices an increased amount of outbound traffic to an unfamiliar IP address. Upon deeper analysis, she found that the traffic consists of sensitive data being transferred. What type of malicious code might be responsible for this?

- (A) Ransomware
- (B) Adware
- (C) **Data Exfiltration Malware**
- (D) Keylogger

Explanation 162. Correct Answer: C. Data Exfiltration Malware. Data Exfiltration Malware is designed to extract and transfer sensitive data from the target system to a location controlled by the attacker. The fact that sensitive data is being transferred to an unfamiliar IP address points to this type of malicious code.

Option A is incorrect. Ransomware is a type of malware that encrypts the victim's files and demands a ransom to restore access. While it might involve data theft, it's primarily known for encryption and ransom demands, not for transferring data outward.

Option B is incorrect. Adware is a type of software that displays unwanted ads on a user's computer. While it might be intrusive and unwanted, it doesn't typically exfiltrate data.

Option D is incorrect. A Keylogger is designed to record keystrokes on a computer and may capture sensitive data like passwords. However, the primary behavior of a keylogger is capturing keystrokes, not transferring large amounts of data outward.

Question 163. During a security assessment of an application, Ryan found that he was able to input larger-than-expected data into a field. Upon doing so, he noticed the application became

unresponsive and eventually crashed. What type of vulnerability might Ryan have uncovered?

- (A) Input Validation Error
- (B) Cross-Site Scripting (XSS)
- (C) **Buffer Overflow**
- (D) Insecure Direct Object Reference (IDOR)

Explanation 163. Correct Answer: C. Buffer Overflow.

Buffer overflow vulnerabilities occur when an application allows more input data than it can securely handle in its allocated buffer space, leading to overwritten adjacent memory. This can lead to application crashes, or potentially, arbitrary code execution by an attacker.

Option A is incorrect. While input validation error can lead to various vulnerabilities, it is a broad category. In the given scenario, the direct consequence of entering larger than expected data is an application crash, which points directly to a buffer overflow.

Option B is incorrect. Cross-Site Scripting (XSS) vulnerabilities allow attackers to inject malicious scripts into web pages viewed by other users. It doesn't cause application crashes due to oversized input.

Option D is incorrect. Insecure Direct Object Reference (IDOR) vulnerabilities occur when an application provides direct access to objects based on user input. It does not cause crashes due to excessive data input.

Question 164. Jake recently ran an old game on his computer that he received from a friend. Shortly after, he discovered that some of his documents were duplicated with slight modifications, and his system's performance was deteriorating. Which kind of malware most likely caused these issues?

- (A) Adware
- (B) Trojan
- (C) Worm
- (D) **Virus**

Explanation 164. Correct Answer: D. Virus. Viruses are malicious programs that attach to clean files and can replicate, leading to multiple instances of themselves. They can modify or corrupt these files and can degrade system performance as they propagate.

Option A is incorrect. Adware primarily focuses on delivering unwanted advertisements to the user. While it can be annoying, it doesn't typically duplicate or modify documents.

Option B is incorrect. Trojans are malicious software that disguises themselves as legitimate programs. While they can perform a variety of malicious actions, they don't self-replicate or modify files in the manner described.

Option C is incorrect. Worms are self-replicating malware that spread across networks. While they can cause performance issues, they don't typically attach to files and modify them as viruses do.

Question 165. The IT department of an e-commerce company is configuring access controls for a new online product inventory system. They want the sales team to update the inventory levels and product details but don't want them to access financial data stored in the same system. Which access control principle is the IT department applying?

- (A) Least Privilege
- (B) **Role-Based Access Control (RBAC)**
- (C) Mandatory Access Control (MAC)
- (D) User-Based Access Control (UBAC)

Explanation 165. Correct Answer: B. Role-Based Access Control (RBAC). Role-Based Access Control (RBAC) assigns permissions based on roles within an organization. Individuals are then assigned roles, and the permissions associated with that role determine what they can and cannot access. In this scenario, the sales team would be given a role that allows them to update inventory but restricts access to financial data.

Option A is incorrect. While the principle of Least Privilege dictates that users should only be given the minimal necessary access to perform their tasks, the scenario specifically focuses on roles (sales team) and the permissions associated with that role, which aligns more with RBAC.

Option C is incorrect. Mandatory Access Control (MAC) uses labels (e.g., classification levels) to determine access. It's more rigid than RBAC and isn't described in the given scenario.

Option D is incorrect. User-Based Access Control (UBAC) assigns permissions directly to each user, rather than based on

their role. The scenario emphasizes role-based permissions, making RBAC the appropriate choice.

Question 166. The IT team at a manufacturing company is deploying an IoT-based monitoring system for their machinery. They want to ensure that these IoT devices, if compromised, cannot adversely affect their main corporate network. What should they implement to achieve this?

- (A) Install antivirus software on all IoT devices
- (B) Regularly patch and update the IoT device firmware
- (C) **Place the IoT devices on a dedicated VLAN**
- (D) Enable multi-factor authentication for IoT devices

Explanation 166. Correct Answer: C. Place the IoT devices on a dedicated VLAN. Placing the IoT devices on a dedicated VLAN (Virtual Local Area Network) provides network isolation, ensuring that the devices are segregated from the main corporate network. This strategy ensures that if an IoT device is compromised, it doesn't pose a direct threat to the core corporate network systems.

Option A is incorrect. Many IoT devices may not support traditional antivirus software, and even if they do, this doesn't achieve the network isolation desired.

Option B is incorrect. While regularly patching and updating device firmware is crucial for security, it doesn't provide network isolation from the main corporate network.

Option D is incorrect. Enabling multi-factor authentication can enhance the security of devices but doesn't provide the network isolation specified in the scenario.

Question 167. A cloud-based collaboration tool used by a company displays a warning to a user stating, "You are logged in from two locations." However, the user has only one active session on their workstation. What should be the primary concern for the security team?

- (A) The user might be using multiple devices
- (B) There's a potential misconfiguration in the tool's settings
- (C) The collaboration tool is facing an outage
- (D) **There might be unauthorized access to the user's account**

Explanation 167. Correct Answer: D. There might be unauthorized access to the user's account. Warnings of concurrent sessions, especially when the user is certain they're using only one device, are red flags for potential unauthorized access. The security team should treat this as a priority and investigate for signs of a breach.

Option A is incorrect. While users often use multiple devices, the scenario mentions the user is certain they have only one active session, making this option unlikely.

Option B is incorrect. While misconfigurations can cause various issues, they don't typically manifest as false concurrent session warnings.

Option C is incorrect. An outage in the collaboration tool would not typically cause a false warning of multiple active sessions.

Question 168. The IT department of a software development company wants to ensure that only company-approved development tools can be executed in their development environment, preventing any unauthorized or potentially harmful software from running. What should the IT department employ to achieve this?

- (A) Implement network segmentation
- (B) Conduct regular vulnerability assessments
- (C) Install a stateful firewall
- (D) **Establish an application allow list**

Explanation 168. Correct Answer: D. Establish an application allow list. Establishing an application allow list would ensure that only specific, pre-approved applications can run in the development environment. This would prevent any unauthorized or potentially malicious software from being executed, aligning directly with the company's goal.

Option A is incorrect. While network segmentation can isolate different parts of the network and limit the spread of potential threats, it does not prevent unauthorized applications from running within a segment.

Option B is incorrect. Regular vulnerability assessments identify weaknesses in systems, but they don't proactively prevent specific applications from running.

Option C is incorrect. A stateful firewall monitors the state of active connections and can block or allow traffic based on stateful parameters, but it doesn't regulate which applications can be executed on a workstation.

Question 169. A large law firm has a centralized document repository where lawyers store client information, legal drafts, and other sensitive data. A new paralegal, Jenna, joins the firm and needs to be able to view client documents but should not be able to modify or delete them. Which type of permission should be granted to Jenna?

- (A) **Read-Only**
- (B) Full Control
- (C) Modify
- (D) Execute

Explanation 169. Correct Answer: A. Read-Only. The Read-Only permission allows users to view and open files or resources but does not allow them to modify, delete, or execute them. In this scenario, granting Jenna Read-Only access ensures she can view client documents without making any alterations or deletions.

Option B is incorrect. Full Control would give Jenna the ability to modify, delete, and even change the permissions of the documents, which exceeds the necessary permissions for her role.

Option C is incorrect. The Modify permission allows a user to make changes to documents, which is not appropriate for Jenna based on the scenario's requirements.

Option D is incorrect. Execute permission is typically related to running programs or scripts and is not relevant to Jenna's need to view documents.

Question 170. A company is developing a new web application that will be processing highly sensitive user data. They want to ensure that if the web server is compromised, attackers cannot directly access the database or other critical infrastructure. Which of the following is the BEST strategy to achieve this objective?

- (A) Use strong authentication methods for the web application
- (B) Encrypt the user data at rest and in transit
- (C) **Place the web server and the database server in separate network segments**
- (D) Implement real-time monitoring of the web server

Explanation 170. Correct Answer: C. Place the web server and the database server in separate network segments. By placing the web server and the database server in separate network segments, the company can achieve isolation. This means that even if the web server is compromised, attackers would still have to breach additional security measures to access the database server or other critical parts of the infrastructure.

Option A is incorrect. While using strong authentication methods is important, it doesn't provide isolation between the web server and other critical components.

Option B is incorrect. Encrypting user data is essential for data protection, but it doesn't provide network-based isolation between the web server and other systems.

Option D is incorrect. Real-time monitoring can provide alerts on suspicious activities, but it doesn't provide the desired isolation.

Question 171. An IT technician is performing a routine security audit of a company's server room. She discovers a server with outdated firmware that hasn't been updated for two years. What potential vulnerability does the outdated firmware expose the server to?

- (A) SQL Injection
- (B) Physical tampering
- (C) **Unpatched exploits**
- (D) Credential stuffing

Explanation 171. Correct Answer: C. Unpatched exploits.

Firmware, like software, receives updates to fix known vulnerabilities. If firmware is outdated, it can leave systems susceptible to known vulnerabilities that attackers can exploit.

Firmware serves as the foundational software for hardware devices. When firmware is not updated regularly, it may contain vulnerabilities that were patched in later versions. These vulnerabilities can potentially be exploited by attackers, putting the device and connected systems at risk.

Option A is incorrect. SQL Injection is a vulnerability associated with databases and web applications, not firmware.

Option B is incorrect. Physical tampering pertains to someone physically accessing and altering a device. While firmware vulnerabilities can sometimes lead to physical tampering (through boot-level attacks), the direct link between outdated firmware and physical tampering is not as strong as the link to unpatched exploits.

Option D is incorrect. Credential stuffing is an attack method that involves using known username-password pairs to gain unauthorized access. It isn't directly related to firmware vulnerabilities.

Question 172. The IT department of a large organization receives reports from employees that they are unable to access certain resources on the network. Upon investigation, the IT department discovers that the Access Control List (ACL) settings have been recently modified. Which of the following would be the PRIMARY reason to review and modify the ACL settings?

- (A) To balance the network load
- (B) To update the organization's firewall rules.
- (C) **To ensure appropriate access rights to resources**
- (D) To update the organization's password policy

Explanation 172. Correct Answer: C. To ensure appropriate access rights to resources. ACLs are essential tools in determining who has access to which resources within a network or system. Regularly reviewing and modifying the ACL settings ensures that users have the appropriate access rights, preventing unauthorized access and ensuring that authorized users can access the resources they need.

Option A is incorrect. While network load balancing is crucial, it is not directly related to ACLs. ACLs focus on access control, not traffic distribution.

Option B is incorrect. Firewall rules are different from ACLs. While they can work together, firewall rules primarily focus on allowing or blocking network traffic, while ACLs determine access permissions to resources.

Option D is incorrect. While updating the organization's password policy is a vital security measure, it is not related to ACLs, which control access to resources based on user or group permissions.

Question 173. You are a security consultant for a company that uses a cloud-based infrastructure. During a security review, you discover that there are no boundaries defined between the company's development, testing, and production environments in the cloud. This can lead to unintended interactions and data leaks. What kind of vulnerability is this scenario illustrating?

- (A) Insecure API endpoints
- (B) Weak encryption methods
- (C) **Lack of resource isolation**
- (D) Insufficient backup strategies

Explanation 173. Correct Answer: C. Lack of resource isolation. Cloud-specific vulnerabilities can arise due to the shared nature of the cloud infrastructure. In this scenario, not having boundaries or isolation between different environments like development, testing, and production can lead to vulnerabilities. If there is no proper resource isolation,

malicious code introduced in the development environment could make its way to production or confidential production data might be exposed in testing, leading to potential data breaches.

Option A is incorrect. Insecure API endpoints would pertain to vulnerabilities where APIs used to manage and interact with cloud services are not properly secured.

Option B is incorrect. Weak encryption methods refer to the use of outdated or vulnerable encryption algorithms, which would not directly relate to the mixing of environments.

Option D is incorrect. Insufficient backup strategies would relate to not having adequate data backup and recovery mechanisms, which is a different concern from resource isolation.

Question 174. During a routine security audit, a company discovered an unauthorized wireless access point using the same SSID as the company's official wireless network. Additionally, this rogue access point was configured without any encryption. What type of wireless attack is this scenario most indicative of?

- (A) War Driving
- (B) Wireless Phishing
- (C) Bluejacking
- (D) Evil Twin

Explanation 174. Correct Answer: D. Evil Twin. An "Evil Twin" attack involves setting up a rogue wireless access point

that mimics a legitimate access point. By doing so, an attacker can intercept, monitor, and manipulate the traffic of users who mistakenly connect to the rogue access point.

Option A is incorrect. War Driving involves driving around areas to discover wireless networks and possibly exploit them. It doesn't necessarily involve creating rogue access points.

Option B is incorrect. Wireless Phishing is not a standard term in wireless network security. Phishing generally involves tricking users into revealing sensitive information through deceptive websites or emails.

Option C is incorrect. Bluejacking involves sending unsolicited messages to Bluetooth-enabled devices. It's not related to wireless networks (Wi-Fi).

Question 175. A system administrator notices that an unauthorized user was able to obtain elevated privileges on a server, even though the default account settings were configured correctly. Upon investigation, it was found that the server's operating system had not been updated for several months.

What type of vulnerability was likely exploited?

- (A) Application Misconfiguration
- (B) **OS Patch Management Issue**
- (C) Weak Encryption Algorithm
- (D) Password Reuse Attack

Explanation 175. Correct Answer: B. OS Patch

Management Issue. When operating systems are not regularly updated, they become vulnerable to known exploits that have

since been patched by vendors. An attacker can take advantage of these vulnerabilities to gain unauthorized elevated privileges.

Operating system-based vulnerabilities often arise due to missed patches or updates. Keeping the OS updated is crucial because vendors frequently release patches to address known vulnerabilities. In this case, the lapse in updating the operating system opened a window for attackers to exploit and obtain elevated privileges.

Option A is incorrect. Application Misconfiguration pertains to incorrect settings or configurations in software applications, not operating systems. The scenario does not suggest any issues with application settings.

Option C is incorrect. Weak Encryption Algorithm refers to encryption that can be easily decrypted or broken due to flaws in the algorithm itself. The scenario doesn't mention encryption or decryption problems.

Option D is incorrect. Password Reuse Attack involves an attacker using previously breached passwords to access different accounts. The scenario doesn't indicate password-related issues.

Question 176. A security analyst discovers that an external IP address has been repeatedly trying every possible combination of characters to gain access to the company's VPN portal for the past two days. Which type of password attack is this MOST likely describing?

(A) Password Spraying

- (B) Dictionary Attack
- (C) Rainbow Table Attack
- (D) **Brute Force Attack**

Explanation 176. Correct Answer: D. Brute Force Attack. A Brute Force Attack involves systematically trying every possible combination of characters until the correct one is found. The scenario specifies that every possible combination of characters is being tried on the VPN portal, indicating a brute force attack.

Option A is incorrect. Password Spraying involves trying a few commonly used passwords across multiple accounts, rather than all possible combinations on one account.

Option B is incorrect. A Dictionary Attack uses a list of common or previously used passwords to attempt access. It doesn't involve trying every possible combination.

Option C is incorrect. A Rainbow Table Attack uses precomputed tables for reversing cryptographic hash functions. This scenario doesn't mention hash values or the use of such tables.

Question 177. Jane, an employee at XYZ Corp, recently noticed that her browser homepage changed unexpectedly, and she's receiving an increasing number of targeted advertisements. Additionally, there's a new toolbar in her browser that she doesn't remember installing. Based on these symptoms, which type of malware is most likely affecting Jane's computer?

- (A) Ransomware
- (B) Worm
- (C) **Spyware**
- (D) Botnet

Explanation 177. Correct Answer: C. Spyware. Spyware is a type of malware that covertly collects information from a user's system. Changes to browser settings, such as a new homepage or a new toolbar, combined with targeted advertisements, are common indicators that spyware might be present on a system.

Option A is incorrect. Ransomware is malware that encrypts a user's files and demands payment for their release. The described symptoms do not align with ransomware behavior.

Option B is incorrect. Worms are a type of malware that self-replicate and spread across networks. They typically don't modify browser settings or show targeted advertisements.

Option D is incorrect. A botnet involves a collection of internet-connected devices, which may have been infected with malware, being used to perform coordinated tasks. It doesn't directly result in the browser-based symptoms described.

Question 178. A software developer at XYZ Corp included a piece of code in the company's software that would corrupt the application's databases if his name was ever removed from the list of contributors in the application credits. Months after he left the company, the application databases were corrupted after an update. What type of malware was responsible for this action?

- (A) Trojan
- (B) Spyware
- (C) Adware
- (D) **Logic bomb**

Explanation 178. Correct Answer: D. Logic bomb. A logic bomb is a type of malware that is triggered by a specific event or condition. In this case, the software developer's name being removed from the contributors triggered the malicious code.

Option A is incorrect. A Trojan disguises itself as legitimate software but performs malicious activities once installed. The scenario does not describe behavior characteristic of a Trojan.

Option B is incorrect. Spyware is designed to collect and send information, typically without the user's knowledge. It does not corrupt databases based on specific triggers.

Option C is incorrect. Adware delivers unwanted advertisements to the user. It does not take malicious actions based on specific events.

Question 179. A popular online shopping platform noticed that some product reviews contained a strange link which, when clicked, led users to a site that resembled the platform but harvested login credentials. What vulnerability in the review system might have allowed attackers to post such links?

- (A) Session Hijacking
- (B) **Cross-site scripting (XSS)**
- (C) Password Spraying
- (D) Credential Stuffing

Explanation 179. Correct Answer: B. Cross-site scripting (XSS). XSS vulnerabilities allow attackers to inject malicious scripts into web content. If the platform's review system does not properly sanitize input, it could permit attackers to embed malicious links that lead to phishing sites.

Cross-site scripting attacks exploit vulnerabilities in web applications to insert malicious scripts. In this case, the ability to post malicious links within product reviews is an indication of an XSS vulnerability. When unsuspecting users click on these links, they are redirected to phishing sites designed to steal their credentials.

Option A is incorrect. Session Hijacking involves taking over an active user session. It doesn't involve posting malicious links in website content.

Option C is incorrect. Password Spraying involves attempting to authenticate against many user accounts with a few commonly used passwords. It doesn't involve embedding malicious links in website content.

Option D is incorrect. Credential Stuffing attacks involve automated attempts to gain access using large sets of valid usernames and passwords. It isn't related to the insertion of malicious links in web content.

Question 180. During a routine security review, a security analyst discovers multiple failed login attempts to a secure server room's electronic access control system, all within a short time span. The access logs show a sequential pattern of

access codes being tried. What type of physical attack is likely being attempted?

- (A) Tailgating
- (B) Phishing
- (C) **Brute force**
- (D) Social engineering

Explanation 180. Correct Answer: C. Brute force. A brute force attack involves trying every possible combination in an attempt to find the correct one. The sequential pattern of access codes being tried in the logs suggests that the attacker is systematically going through all potential combinations.

Option A is incorrect. Tailgating involves an attacker following an authorized person into a secure area without the proper credentials. It doesn't involve multiple electronic access code attempts.

Option B is incorrect. Phishing is a type of social engineering attack that typically involves tricking someone into divulging their credentials or other sensitive information. It doesn't involve direct physical access attempts.

Option D is incorrect. While social engineering does involve manipulating individuals to gain unauthorized access, it is not specific to a brute force attack on an electronic system.

Question 181. A multinational corporation communicates sensitive information between its branches using encryption. An internal audit reveals that the encryption algorithms being used are those that were deprecated several years ago. Which of the

following cryptographic vulnerabilities is the organization most exposed to?

- (A) Key generation flaw
- (B) **Weak algorithms susceptible to attacks**
- (C) Inadequate public key infrastructure
- (D) Mismanagement of cryptographic keys

Explanation 181. Correct Answer: B. Weak algorithms susceptible to attacks. When an organization is found to be using deprecated or older encryption algorithms, it means they are relying on cryptographic methods that might have known vulnerabilities or could be easier to break due to advancements in computing and cryptanalysis. Over time, certain algorithms are found to have weaknesses and are replaced with more robust ones.

Option A is incorrect. The scenario does not specify issues with key generation but rather focuses on the use of outdated encryption algorithms.

Option C is incorrect. There's no information in the scenario suggesting problems with the organization's public key infrastructure.

Option D is incorrect. While key management is crucial, the primary issue presented in the scenario revolves around the usage of weak or outdated algorithms.

Question 182. During a routine audit of the corporate servers, the system administrator discovers that a week's worth of security logs are missing from one of the key application

servers. Which of the following is the MOST likely reason for this occurrence?

- (A) The logging service experienced a malfunction
- (B) There was insufficient storage space for the logs
- (C) **A malware attack aimed to erase traces of intrusion**
- (D) The time zone setting was incorrectly configured

Explanation 182. Correct Answer: C. A malware attack aimed to erase traces of intrusion. One of the primary tactics attackers use after gaining unauthorized access is to cover their tracks. Deleting or altering logs is a common method used to avoid detection and prevent any trace of malicious activity.

Option A is incorrect. While it's possible for the logging service to malfunction, it's less likely for it to result in a specific week's worth of logs being missing, without affecting other time periods.

Option B is incorrect. Insufficient storage space can cause newer logs to overwrite older ones, but it would typically not result in a discrete chunk of logs, such as an entire week, to be missing.

Option D is incorrect. A misconfigured time zone setting might cause timestamp discrepancies in logs, but it wouldn't cause logs to be missing.

Question 183. The content filtering logs at a retail company display multiple instances of blocked access to a file download URL ending with “.exe”. The source IP address belongs to a point of sale (POS) terminal. What should be the primary

concern for the security team?

- (A) The POS terminal might have outdated software
- (B) There's a possible misconfiguration in the content filtering rules
- (C) **The POS terminal might be compromised and trying to download malicious executables**
- (D) The company's internet speed is too slow

Explanation 183. Correct Answer: C. The POS terminal might be compromised and trying to download malicious executables.

POS terminals shouldn't be downloading executable files from the internet, especially without administrative oversight. Multiple attempts to download ".exe" files could indicate that the POS terminal is compromised and that malicious software is attempting to download further payloads.

Option A is incorrect. While outdated software is a security concern, it wouldn't manifest as multiple blocked attempts to download executables.

Option B is incorrect. Misconfigurations in content filtering rules might block legitimate content, but the specific action of a POS terminal trying to download executable files is suspicious regardless of content filtering rules.

Option D is incorrect. The company's internet speed has no relevance to the specific content being blocked by the filtering system

Question 184. Kara, a financial analyst, began to notice unusual account activity tied to her credentials. She is sure she hasn't initiated these transactions. Upon further investigation, IT discovered a program on her computer that was recording her keystrokes. What type of malware was found on Kara's computer?

- (A) Ransomware
- (B) **Keylogger**
- (C) Adware
- (D) Rootkit

Explanation 184. Correct Answer: B. Keylogger. A keylogger is a type of malicious software designed to capture and record the keystrokes of a user without their knowledge, often leading to unauthorized access to sensitive information such as usernames, passwords, and other confidential details.

Option A is incorrect. Ransomware is malware that encrypts a user's data and demands payment for its decryption. It doesn't record keystrokes.

Option C is incorrect. Adware delivers unwanted ads to the user. It doesn't record keystrokes.

Option D is incorrect. A rootkit provides stealthy access to a computer, allowing an attacker to maintain privileged access without detection. It doesn't specifically record keystrokes.

Question 185. A finance department employee, Maya, is transferred to the HR department. The IT department is considering her access requirements. Which of the following

actions aligns best with the principle of least privilege?

- (A) Retain Maya's access to the finance system and grant additional access to the HR system
- (B) Remove all previous access rights and provide her access solely to the HR system**
- (C) Grant Maya administrative rights to ease her transition between departments
- (D) Limit Maya's access to read-only for both finance and HR systems for a transitional period

Explanation 185. Correct Answer: B. Remove all previous access rights and provide her access solely to the HR system.

When an employee transitions from one department to another, their access requirements change. To uphold the principle of least privilege, it's essential to re-evaluate and adjust access rights. Maya no longer requires access to the finance system and should only have access to the resources necessary for her new role in HR.

Option A is incorrect. Retaining access to the finance system when Maya no longer works in that department is unnecessary and could be a security risk.

Option C is incorrect. Granting administrative rights is excessive and would provide Maya with more access than necessary for her new role.

Option D is incorrect. While read-only access limits potential damage, providing access to both systems is unnecessary if Maya's new role only requires access to the HR system.

Question 186. During a security audit, a company realized that a malicious actor was able to situate themselves on the network path, capturing TLS handshake messages between clients and the server. The attacker's goal is to weaken the encryption by influencing the cipher suite negotiation process. What type of network attack does this scenario depict?

- (A) ARP Poisoning
- (B) **Downgrade Attack**
- (C) SYN Flood
- (D) Ping of Death

Explanation 186. Correct Answer: B. Downgrade Attack. A Downgrade Attack occurs when an attacker interferes with the setup process (e.g., TLS handshake) to force two entities to settle on a less secure communication mode or encryption standard. In this case, by capturing and potentially altering the TLS handshake messages, the attacker is trying to make the client and server use a weaker cipher suite.

Option A is incorrect. ARP Poisoning is a type of attack where an attacker sends falsified ARP messages over a local area network to link the attacker's MAC address with the IP address of another node (such as the default gateway). This is a way to facilitate on-path attacks, but the scenario describes influencing the cipher suite negotiation, which is a Downgrade Attack.

Option C is incorrect. SYN Flood is a form of denial-of-service attack in which an attacker sends a sequence of SYN requests to a target's system in an attempt to consume server resources. It does not relate to capturing TLS handshake messages.

Option D is incorrect. Ping of Death is an old attack where malicious parties send malformed or oversized ping packets to crash the target system. It doesn't involve capturing or influencing the TLS handshake process.

Question 187. A developer has implemented a new feature on a company's website that allows users to search for products by their names. Within a few days, the IT team noticed abnormal activities where entire tables from the database were being dumped. Which vulnerability might the new feature have introduced?

- (A) Cross-Site Scripting (XSS)
- (B) Distributed Denial-of-Service (DDoS)
- (C) **Structured Query Language injection (SQLi)**
- (D) Cross-Site Request Forgery (CSRF)

Explanation 187. Correct Answer: C. Structured Query Language injection (SQLi). SQLi attacks occur when an attacker can insert or "inject" SQL code into a query. If user input is not properly sanitized before being used in SQL statements, attackers can exploit this to manipulate the queries, which can lead to unauthorized viewing of data, corrupting or deleting data, and other malicious activities.

Structured Query Language injection, or SQLi, is a code injection technique that attackers use to run malicious SQL statements on a database. Given that entire tables from the database were dumped after implementing a search feature, it's a clear indication that the feature did not properly sanitize user input, allowing for SQLi.

Option A is incorrect. Cross-Site Scripting (XSS) attacks inject malicious scripts into web pages viewed by users. It doesn't lead to dumping of database tables as described in the scenario.

Option B is incorrect. Distributed Denial-of-Service (DDoS) attacks overwhelm a target with traffic, causing service interruptions. It's not related to the extraction of database information.

Option D is incorrect. Cross-Site Request Forgery (CSRF) tricks victims into submitting malicious requests. It doesn't result in the dumping of database tables.

Question 188. During a routine security assessment, Jake, a penetration tester, discovers that by modifying a configuration file located in a public directory, he can assign himself administrative privileges in the application. What type of vulnerability is Jake exploiting?

- (A) Cross-Site Scripting (XSS)
- (B) **Privilege Escalation**
- (C) SQL Injection
- (D) Insecure Direct Object Reference (IDOR)

Explanation 188. Correct Answer: B. Privilege Escalation.

Privilege escalation occurs when a user increases their privileges beyond what was originally granted to them, allowing them to perform actions that they should not be allowed to. In this scenario, Jake is elevating his privileges in the application by modifying a configuration file, indicating a privilege escalation vulnerability.

Option A is incorrect. Cross-Site Scripting (XSS) involves an attacker injecting malicious scripts into web content viewed by other users. This scenario does not relate to injecting scripts.

Option C is incorrect. SQL Injection vulnerabilities allow attackers to manipulate or query a database directly through input fields. The scenario does not indicate any interaction with a database.

Option D is incorrect. Insecure Direct Object Reference (IDOR) vulnerabilities occur when an application allows access to objects based on user-supplied input. While the scenario involves accessing a file, it is the act of elevating privileges that is the primary concern.

Question 189. An organization's security team discovered that an attacker had gained unauthorized access to a server. Upon investigating, they found a software tool that allowed the attacker to mask processes, files, and system data, effectively remaining hidden while maintaining privileged access. What type of malware was implanted by the attacker?

- (A) Trojan
- (B) Worm
- (C) Logic Bomb
- (D) **Rootkit**

Explanation 189. Correct Answer: D. Rootkit. A rootkit is malware that provides stealthy access to a computer and hides its presence from standard detection methods. It can mask files, processes, and other system data.

Option A is incorrect. A Trojan disguises itself as legitimate software but performs malicious activities once installed. It does not inherently hide processes or files.

Option B is incorrect. Worms are malware that can replicate themselves to spread to other systems. They don't typically hide their activities at the system level.

Option C is incorrect. A logic bomb is set to execute its malicious activity when a specific event or condition occurs. It doesn't focus on hiding system data or processes.

Question 190. The IT team of XYZ Corp received an alert that an employee's account was used to access the company's portal from Paris at 2:00 PM and then from Tokyo at 2:30 PM. The employee is currently on a business trip to Paris. What could this alert be indicating?

- (A) The employee quickly traveled from Paris to Tokyo
- (B) The company's time zone settings are misconfigured
- (C) There's a possible VPN misconfiguration on the employee's computer
- (D) **The employee's account might have been compromised**

Explanation 190. Correct Answer: D. The employee's account might have been compromised. Impossible travel, in this context, refers to the improbable nature of someone being in two distant geographical locations within a short time frame. Given the close time proximity of both access attempts, it's highly improbable that the employee traveled from Paris to

Tokyo in half an hour. This is a common indicator of account compromise.

Option A is incorrect. It's virtually impossible for someone to travel from Paris to Tokyo in just 30 minutes.

Option B is incorrect. Time zone misconfigurations might cause timestamp discrepancies, but they wouldn't cause the appearance of logins from two distant cities within such a short time frame.

Option C is incorrect. Even if there's a VPN misconfiguration, it would not explain the access from two very different geographical locations in such a short span of time.

Question 191. An organization recently deployed a cloud-based database to support its new application. A few weeks later, unauthorized access to the database was detected. An investigation revealed that the database was accessible without a password. Which of the following misconfigurations is primarily responsible for the security breach?

- (A) **Default configurations left unchanged**
- (B) Insufficient network segmentation
- (C) Encryption not enabled at rest
- (D) Lack of intrusion detection system

Explanation 191. Correct Answer: A. Default configurations left unchanged. The scenario describes a situation where a cloud-based database was accessible without a password. This is a common oversight when default configurations, which may

have no password or a widely known default password, are left unchanged upon deployment.

Option B is incorrect. While network segmentation is crucial for security, the primary issue in this scenario is the database's lack of password protection, not its network placement.

Option C is incorrect. Though encryption at rest is a best practice for data protection, the immediate issue here is unauthorized access due to a lack of password, not data exposure from the database's stored data.

Option D is incorrect. An intrusion detection system (IDS) might have detected the unauthorized access sooner, but the core vulnerability was the unchanged default configurations.

Question 192. A user reports that whenever they try to visit their online banking website, they are redirected to a website that looks identical but has a slightly different URL. The fake website asks for additional personal details that the bank never requested before. Which type of DNS attack is the user likely encountering?

- (A) DNS Tunneling
- (B) DNS Fast Flux
- (C) **DNS Cache Poisoning**
- (D) Domain Hijacking

Explanation 192. Correct Answer: C. DNS Cache Poisoning. DNS Cache Poisoning, also known as DNS spoofing, involves corrupting the DNS cache data in DNS resolvers to redirect

users to malicious websites instead of the actual intended websites.

Option A is incorrect. DNS Tunneling is a technique where non-DNS traffic is encapsulated in DNS protocols. It's a way to bypass network security but doesn't usually lead to the described redirection scenario.

Option B is incorrect. DNS Fast Flux involves rapidly changing the IP address associated with a domain name to hide the malicious server behind it. It is used to prevent the malicious domain from being taken down but doesn't cause redirection to a similar-looking site.

Option D is incorrect. Domain Hijacking involves an attacker taking control of a domain by altering its registration data without the owner's permission. While this could lead to a similar outcome, the scenario describes a situation where only certain users are redirected, not all visitors to the domain.

Question 193. Alex recently purchased a new laptop. Upon first startup, he noticed multiple pre-installed software applications, most of which he didn't recognize or find necessary. The laptop's performance was slower than expected given its hardware specifications. Which type of software is most likely causing this performance degradation?

- (A) Ransomware
- (B) Bloatware
- (C) Spyware
- (D) Adware

Explanation 193. Correct Answer: B. Bloatware. Bloatware refers to unnecessary software applications that come pre-installed on new computers. These applications often consume system resources, leading to reduced performance.

Manufacturers sometimes pre-install these applications for promotional purposes or due to partnerships with software providers.

Option A is incorrect. Ransomware encrypts a user's files and demands payment for their decryption. It doesn't come pre-installed on new computers.

Option C is incorrect. Spyware covertly collects information from a system without the user's knowledge. It doesn't typically come pre-installed on new devices as bloatware does.

Option D is incorrect. Adware automatically displays or downloads advertising material on a computer. While it might be annoying, it's not typically pre-installed software that comes with new computers aimed at degrading performance.

Question 194. The IT department of a large corporation is performing a vulnerability assessment on its virtualized infrastructure. They come across a potential threat where a user from within a VM can interact and possibly compromise the host system. What is this type of vulnerability commonly referred to as?

- (A) VM cloning
- (B) VM snapshotting
- (C) **VM escape**
- (D) VM migration

Explanation 194. Correct Answer: C. VM escape. A VM escape occurs when an attacker runs code on a VM that allows them to break out of the VM's isolated environment and gain access to the host system.

A virtual machine (VM) escape refers to the exploitation of a vulnerability in the virtualization software, allowing an attacker who has control over a VM to break out of its isolated environment and gain access to the host system. This can lead to the potential compromise of other VMs running on the same host or the underlying infrastructure.

Option A is incorrect. VM cloning is the process of creating an exact copy of a VM. It does not involve breaking out of the VM's isolated environment.

Option B is incorrect. VM snapshotting involves creating a point-in-time copy of a VM, which can be used for backup or recovery purposes. It is not related to escaping from a VM.

Option D is incorrect. VM migration refers to the process of moving a VM from one host to another, often for load balancing or hardware maintenance. It does not involve escaping from the VM's isolated environment.

Question 195. A renowned technology company recently released a new line of routers. After a short period, security researchers discovered that some of these routers contain malicious chips embedded during the manufacturing process. This incident most likely represents a vulnerability related to which supply chain aspect?

- (A) Outsourced software development risks
- (B) Service provider's outdated security practices
- (C) **Hardware provider's embedded compromise**
- (D) Inadequate vendor background checks

Explanation 195. Correct Answer: C. Hardware provider's embedded compromise. Supply chain vulnerabilities in the context of hardware providers can involve the introduction of malicious components or chips during the manufacturing process. In this scenario, the presence of malicious chips in the routers is a direct reflection of a vulnerability due to a compromised hardware provider.

Option A is incorrect. The scenario revolves around a hardware compromise, not software development outsourcing.

Option B is incorrect. While it's essential for service providers to employ up-to-date security practices, the vulnerability in this scenario is attributed to a hardware compromise and not outdated security practices.

Option D is incorrect. Although vendor background checks are important, this scenario emphasizes a vulnerability stemming from the hardware manufacturing process, not the vetting process of vendors.

Question 196. A large news website was rendered unavailable during a major news event. Network logs show an overwhelming amount of traffic from IoT devices. Which type of DDoS attack leveraged IoT devices is this indicative of?

- (A) Reflected Attack

- (B) **Botnet Attack**
- (C) Amplification Attack
- (D) Teardrop Attack

Explanation 196. Correct Answer: B. Botnet Attack. Botnets, which are networks of compromised devices (including IoT devices), are often used to conduct large-scale DDoS attacks by directing the combined bandwidth of the devices towards a target.

Option A is incorrect. In a reflected attack, an attacker sends traffic to a third party, disguising it as if it came from the victim, which then reflects the traffic to the victim. It doesn't primarily involve IoT devices.

Option C is incorrect. An amplification attack leverages vulnerable network services to amplify the amount of traffic sent to a victim. The primary focus isn't the use of IoT devices.

Option D is incorrect. A teardrop attack involves sending mangled IP fragments with overlapping and oversized payloads to crash a target system. It doesn't specifically utilize IoT devices.

Question 197. A web application requires users to authenticate using a token sent to their email. Alex, a security analyst, observes that once logged in, if he presents the same token again, he is granted access without any restrictions. What type of vulnerability does this situation depict?

- (A) Cross-Site Request Forgery (CSRF)
- (B) **Replay Attack**

- (C) Man-in-the-Middle (MitM) Attack
- (D) Cross-Site Scripting (XSS)

Explanation 197. Correct Answer: B. Replay Attack. A replay attack, also known as playback attack, occurs when an attacker intercepts data and then retransmits it. In this scenario, Alex was able to reuse the authentication token to gain access, indicating that the system does not have mechanisms in place to prevent replayed tokens from being accepted multiple times.

Option A is incorrect. Cross-Site Request Forgery (CSRF) is an attack where an attacker tricks the victim into performing unwanted actions on a web application where they're authenticated. It doesn't involve reusing authentication tokens.

Option C is incorrect. While a Man-in-the-Middle (MitM) Attack can involve intercepting data between two parties, the described scenario doesn't involve an attacker modifying or relaying the information in real-time.

Option D is incorrect. Cross-Site Scripting (XSS) vulnerabilities allow attackers to inject malicious scripts into web pages. The scenario doesn't indicate any script injection.

Question 198. Liam, a security analyst, is investigating a potential breach. He discovers that a malicious actor sent requests to the server by altering HTTP headers to impersonate another user, thereby gaining unauthorized access. Which type of application attack is this?

- (A) Cross-Site Request Forgery (CSRF)
- (B) Cross-Site Scripting (XSS)

- (C) HTTP Header Forgery
- (D) Session Hijacking

Explanation 198. Correct Answer: C. HTTP Header Forgery. HTTP Header Forgery involves manipulating HTTP headers in a request to impersonate, spoof, or deceive systems, often for bypassing security controls or impersonating other users. In the described scenario, the malicious actor altered HTTP headers to impersonate another user, indicating an HTTP Header Forgery attack.

Option A is incorrect. Cross-Site Request Forgery (CSRF) involves tricking a user into executing actions on a web application where they're authenticated, without their knowledge. While it involves forgery, it doesn't involve directly manipulating HTTP headers as described.

Option B is incorrect. Cross-Site Scripting (XSS) involves injecting malicious scripts into web content viewed by other users. The scenario does not pertain to injecting scripts.

Option D is incorrect. Session Hijacking involves taking over a user's session to perform unauthorized actions. It doesn't specifically involve the manipulation of HTTP headers.

Question 199. A company's network administrator notices that several switches in the network infrastructure are no longer receiving firmware updates from the manufacturer. These devices are no longer sold or supported. What vulnerability do these switches introduce to the network?

- (A) Physical hardware tampering

- (B) Lack of redundancy
- (C) **Increased susceptibility to new threats**
- (D) Wireless interference

Explanation 199. Correct Answer: C. Increased susceptibility to new threats. End-of-life hardware often does not receive security updates or patches, making them more vulnerable to new and evolving threats over time.

End-of-life (EOL) hardware refers to devices that are no longer supported by their manufacturers. This lack of support means that the devices won't receive any further security updates, patches, or technical support. Consequently, these devices become more susceptible to new threats and vulnerabilities, posing a security risk to the network.

Option A is incorrect. End-of-life status doesn't inherently make a device more vulnerable to physical tampering. However, without ongoing updates, they might be susceptible to firmware or software-based attacks, which could lead to physical tampering in some scenarios.

Option B is incorrect. Lack of redundancy refers to a single point of failure in a system or network. It is not directly related to the vulnerabilities associated with EOL hardware.

Option D is incorrect. Wireless interference is related to the disruption of wireless signals and is not a direct consequence of EOL hardware.

Question 200. While reviewing web server logs, Sarah, a security analyst, notices a pattern of requests containing “../%2F..” in the URLs. She suspects this might be an attempt to exploit a vulnerability. Which type of application attack is likely being attempted?

- (A) Command Injection
- (B) Cross-Site Scripting (XSS)
- (C) **Directory Traversal**
- (D) Cross-Site Request Forgery (CSRF)

Explanation 200. Correct Answer: C. Directory Traversal.

Directory traversal (also known as path traversal) involves manipulating variables referencing files with “../” sequences and its variations (like “../%2F..”, which URL-decodes to “../..”) to navigate outside of the intended directory. This can allow an attacker to access restricted files on the web server. The pattern Sarah observed in the logs indicates a directory traversal attack attempt.

Option A is incorrect. Command injection attacks involve executing arbitrary commands on the server via application vulnerabilities. The specific pattern observed in the logs does not suggest command execution.

Option B is incorrect. Cross-Site Scripting (XSS) attacks involve injecting malicious scripts into web pages viewed by other users. The pattern observed doesn’t pertain to script injection.

Option D is incorrect. Cross-Site Request Forgery (CSRF) tricks victims into submitting a malicious request. It does not

involve directory or path manipulation as described in the scenario.

Question 201. A security analyst is reviewing network logs and notices that an attacker positioned in between the user and the target website is intercepting and potentially modifying the user's communications before passing them on to the intended destination. This malicious activity occurs transparently, with neither the user nor the target website being aware. What type of network attack is being described?

- (A) Replay Attack
- (B) Smurf Attack
- (C) **On-path Attack**
- (D) Spoofing Attack

Explanation 201. Correct Answer: C. On-path Attack. An On-path Attack, also known as a Man-in-the-Middle (MitM) attack, involves an attacker intercepting communications between two parties, potentially modifying the communication, and then relaying it to the intended recipient. Both the source and the destination are unaware of the attacker's presence.

Option A is incorrect. A Replay Attack involves capturing legitimate data packets and retransmitting them at a later time to create an unauthorized effect. It doesn't involve active interception and modification in real-time.

Option B is incorrect. A Smurf Attack is a type of denial-of-service attack that uses ICMP Echo (ping) traffic to flood a target system. It has no relation to intercepting and modifying user communications.

Option D is incorrect. Spoofing Attack involves pretending to be something or someone else. While on-path attacks might involve some elements of spoofing, the specific action described in the scenario is more aligned with an on-path attack.

Question 202. A financial firm outsources its payment processing to a third-party service provider. After a series of fraudulent transactions, it was discovered that the service provider was not employing the latest encryption standards when transmitting data. Which vulnerability related to supply chain does this scenario highlight?

- (A) Inadequate vendor background checks
- (B) **Service provider's outdated security practices**
- (C) Deficient hardware components from a supplier
- (D) Software with embedded backdoors

Explanation 202. Correct Answer: B. Service provider's outdated security practices. Supply chain vulnerabilities encompass risks originating from third-party vendors and service providers. In this scenario, the third-party service provider's failure to use current encryption standards for transmitting data exemplifies a vulnerability that arises due to outdated security practices by the service provider.

Option A is incorrect. While vendor background checks are essential, the scenario does not specifically point towards a problem with the vendor's background. It focuses on their encryption practices.

Option C is incorrect. The scenario doesn't mention hardware components or any issues related to them.

Option D is incorrect. The issue here pertains to encryption standards, not to software with embedded backdoors.

Question 203. Julia, a cybersecurity analyst, notices a recently installed application named “PhotoEditorPro.exe” on a corporate workstation. Upon further inspection, she identifies that this application is silently exfiltrating sensitive company data to an external IP address. Which type of malware is Julia most likely observing?

- (A) Worm
- (B) Ransomware
- (C) **Trojan**
- (D) Adware

Explanation 203. Correct Answer: C. Trojan. A Trojan is a type of malware that disguises itself as a legitimate software or application. Unlike viruses, Trojans don’t replicate themselves, but they can be just as destructive if not more so. In this case, the “PhotoEditorPro.exe” appears to be a legitimate photo editing application but is actually being used to transmit sensitive data to an external source.

Option A is incorrect. Worms are malware programs that replicate themselves to spread to other devices. They don’t typically disguise themselves as legitimate applications.

Option B is incorrect. Ransomware encrypts the victim’s data and demands a ransom to decrypt it. It doesn’t disguise itself as legitimate software.

Option D is incorrect. Adware is software that displays unwanted advertisements. It doesn't typically exfiltrate data or disguise itself as legitimate software.

Question 204. A company's IT department notices a sharp increase in account lockouts over the past two days, especially during non-business hours. While some accounts are from various departments, a majority are from the finance team. Which of the following is the MOST plausible explanation for these lockouts?

- (A) Scheduled maintenance by the IT department
- (B) Employees are sharing passwords within the finance team
- (C) **An attacker is trying to gain unauthorized access**
- (D) A recent password policy change requiring more frequent changes

Explanation 204. Correct Answer: C. An attacker is trying to gain unauthorized access. A sudden increase in account lockouts, especially during non-business hours, indicates suspicious activity. The targeted nature of the lockouts, especially on sensitive departments like finance, suggests an attacker might be attempting unauthorized access.

Option A is incorrect. Scheduled maintenance would typically be communicated in advance, and it's unlikely to cause a sharp increase in account lockouts.

Option B is incorrect. While employees sharing passwords is a security concern, it would not typically result in a surge of account lockouts, especially during non-business hours.

Option D is incorrect. A password policy change might result in some increased lockouts, but the targeted nature of the lockouts (majority from finance) and their occurrence during non-business hours make this option less likely.

Question 205. Sarah, a software developer at a tech company, decided to gain root access to her company-issued mobile device to customize its features. Soon after, the IT department detected unauthorized data transmissions from her device. Which mobile vulnerability is most likely associated with her actions?

- (A) Side loading of applications
- (B) Inconsistent OS updates
- (C) **Mobile device jailbreaking**
- (D) Use of open Wi-Fi networks

Explanation 205. Correct Answer: C. Mobile device jailbreaking. Jailbreaking is the process of removing the restrictions imposed by the manufacturer on certain devices, thereby allowing root access. With this root access, users can install and customize software that hasn't been approved by the device's manufacturer or carrier. However, jailbreaking can expose the device to various security vulnerabilities, as indicated by unauthorized data transmissions.

Option A is incorrect. Side loading refers to the installation of applications from sources other than the official app store. While side loading can pose security risks, Sarah's actions specifically relate to gaining root access, which points to jailbreaking.

Option B is incorrect. Inconsistent OS updates refer to the presence of various versions of an OS across different devices. Sarah's actions are related to obtaining root access, not inconsistent updates.

Option D is incorrect. Using open Wi-Fi networks can expose mobile devices to threats, but Sarah's vulnerability arose from gaining root access, not from her choice of Wi-Fi networks.

Question 206. After a recent cyber attack on a corporation's central database, the IT department has been tasked with enhancing the security of their network infrastructure. Which of the following would be the BEST technique to ensure that different departments, like HR and Finance, cannot access each other's sensitive data?

- (A) **Implement network segmentation based on departments**
- (B) Upgrade the bandwidth of the entire network
- (C) Use a single strong password for all departments
- (D) Move all department data to the cloud

Explanation 206. Correct Answer: A. Implement network segmentation based on departments. Network segmentation divides a network into multiple segments or subnets, each acting as its own small network. This limits access between segments and can protect sensitive data by ensuring that only those within a segment can access its resources.

Option B is incorrect. While upgrading the bandwidth may improve network speeds, it does not address the security concern of segregating departmental data.

Option C is incorrect. Using a single strong password for all departments does not prevent one department from accessing another's data. It also introduces a single point of failure.

Option D is incorrect. Moving data to the cloud can offer some security benefits, but without proper access controls and segmentation, different departments could still access each other's data.

Question 207. During an organization's security review, the cybersecurity analyst noticed that there were multiple failed login attempts for different user accounts, each with a few commonly used passwords. What type of password attack does this scenario BEST describe?

- (A) Brute Force Attack
- (B) Dictionary Attack
- (C) Credential Stuffing
- (D) **Password Spraying**

Explanation 207. Correct Answer: D. Password Spraying.

Password Spraying is an attack method where the attacker tries a few commonly used passwords against multiple user accounts, rather than trying many passwords against a single account. The scenario described shows multiple user accounts with common passwords being targeted, aligning with this method.

Option A is incorrect. A Brute Force Attack involves trying all possible password combinations for a particular account. The scenario describes trying common passwords on multiple accounts, not exhaustive combinations on one.

Option B is incorrect. A Dictionary Attack involves trying a list of probable passwords, often extracted from dictionaries or common password lists, against a single account. The scenario emphasizes multiple accounts.

Option C is incorrect. Credential Stuffing involves using previously leaked username and password pairs to gain unauthorized access. The emphasis is on using known credentials, not common passwords.

Question 208. The IT team at TechnoCorp has noticed a consistent pattern over the last week where a particular server's CPU usage spikes to 100% between 2:00 AM and 4:00 AM, a time when there's typically minimal user activity. What could be the MOST probable reason for this?

- (A) The server is automatically updating its software
- (B) An employee is running a heavy computational task
- (C) The server is undergoing a DDoS attack
- (D) **Malware is performing cryptomining activities**

Explanation 208. Correct Answer: D. Malware is performing cryptomining activities. Cryptomining malware often causes significant resource consumption, especially CPU usage. Attackers frequently schedule such activities during off-peak hours to reduce the chance of detection. Given the consistent pattern of high CPU usage during off-hours, cryptomining malware is a probable cause.

Option A is incorrect. While software updates can cause resource consumption, they typically don't result in consistent, prolonged 100% CPU usage over multiple days.

Option B is incorrect. Though it's possible an employee might be running a heavy task, the consistent pattern during odd hours makes it less likely compared to malicious activities.

Option C is incorrect. While a DDoS attack can cause resource consumption, it wouldn't specifically target CPU usage consistently during the same timeframe every night.

Question 209. An organization's IT department noticed a rapid increase in network traffic over the past 24 hours.

Simultaneously, many employees reported that their systems have been slow and that they received a file named "updatePatch.exe" from coworkers via email, even though the coworkers did not intentionally send any files. What type of malware is most likely responsible for this behavior?

- (A) Trojan
- (B) Ransomware
- (C) Adware
- (D) **Worm**

Explanation 209. Correct Answer: D. Worm. Worms are a type of malware that self-replicates and spreads to other devices. The rapid increase in network traffic and the distribution of a file to various users without the sender's knowledge is characteristic of worm behavior. They can consume bandwidth and system resources, causing systems to slow down.

Option A is incorrect. A Trojan disguises itself as legitimate software but does not replicate itself or send itself via email like worms do.

Option B is incorrect. Ransomware encrypts files on a victim's computer and demands a ransom for the decryption key. It doesn't self-replicate and spread like a worm.

Option C is incorrect. Adware primarily serves unwanted ads to users and doesn't replicate itself to spread to other systems.

Question 210. During a routine check, an IT technician notices several files on a company server have been renamed with a ".locked" extension and there's a new file named "README_TO_RECOVER_FILES.txt" present in the root directory. Based on these indicators, which type of malicious activity is most likely in progress?

- (A) Worm propagation
- (B) Trojan horse execution
- (C) **Ransomware attack**
- (D) Logic bomb activation

Explanation 210. Correct Answer: C. Ransomware attack.

Ransomware is a type of malicious software that encrypts a victim's files, rendering them inaccessible. The attacker then demands a ransom from the victim in return for the decryption key. The renaming of files with a specific extension (like ".locked") and the presence of a ransom note (like "README_TO_RECOVER_FILES.txt") are typical indicators of a ransomware attack.

Option A is incorrect. Worm propagation refers to the spread of a standalone malware computer program that replicates itself to spread to other computers. It doesn't typically rename files or leave readable messages.

Option B is incorrect. A Trojan horse is malicious software that deceives users about its true intent. While it can deliver a ransomware payload, the described indicators more directly suggest ransomware activity.

Option D is incorrect. A logic bomb is a piece of code that executes a malicious function when certain conditions are met, but it doesn't necessarily leave the described file traces.

Question 211. An organization is choosing a hash function for digital signatures. They want to ensure that it is resistant to scenarios where an attacker might produce two different messages having the same hash. Which type of attack are they trying to defend against?

- (A) Side-channel Attack
- (B) Replay Attack
- (C) **Birthday Attack**
- (D) Ciphertext-only Attack

Explanation 211. Correct Answer: C. Birthday Attack. In a Birthday Attack, attackers exploit the mathematics behind the birthday problem in probability theory, aiming to find two different inputs that produce the same output, or hash. When selecting a hash function for digital signatures, it's crucial to pick one that is resistant to Birthday Attacks to maintain the integrity of the signatures.

Option A is incorrect. A Side-channel Attack involves obtaining information from the physical implementation of a cryptographic system rather than exploiting a theoretical weakness in algorithms or protocols. It's unrelated to producing two messages with the same hash.

Option B is incorrect. A Replay Attack involves intercepting data (like a login session) and then resending or replaying it to gain unauthorized access. It does not focus on matching hash values.

Option D is incorrect. In a Ciphertext-only Attack, the attacker has the ciphertext and tries to derive the plaintext without knowing the key. The scenario does not describe this type of attack.

Question 212. An IT security team received reports that a new, previously unknown vulnerability was being actively exploited in the wild. The software vendor has not yet provided a patch for the vulnerability. What is the most accurate term for this vulnerability?

- (A) Legacy vulnerability
- (B) **Zero-day vulnerability**
- (C) Patched vulnerability
- (D) Known vulnerability

Explanation 212. Correct Answer: B. Zero-day vulnerability. A zero-day vulnerability refers to a flaw in software, hardware, or firmware that is unknown to the vendor. This type of vulnerability is a risk because there is no fix or

patch for it at the time of discovery, and it may already be actively exploited by malicious actors.

Option A is incorrect. A legacy vulnerability typically refers to a vulnerability in older software or systems that might not be supported anymore, not necessarily an unknown and unpatched flaw.

Option C is incorrect. A patched vulnerability implies that there's already a fix available for the flaw. In the scenario provided, no patch has been released yet.

Option D is incorrect. While the vulnerability may become known to some entities, such as the security team in this scenario, it remains unknown to the software vendor. Thus, "known vulnerability" is not the most accurate descriptor in this context.

Question 213. A company has recently deployed a new e-commerce application. The security team wants to ensure they can detect any unauthorized or malicious activities on the application. Which of the following would be the MOST effective way to achieve this goal?

- (A) Conduct a penetration test on the application
- (B) Install a firewall in front of the application
- (C) **Implement continuous monitoring of the application's logs and activities**
- (D) Provide training to users about secure browsing habits

Explanation 213. Correct Answer: C. Implement continuous monitoring of the application's logs and activities.

Continuous monitoring of an application's logs and activities allows the security team to detect and respond to any suspicious or unauthorized behavior in real-time. This ensures that potential threats can be identified and addressed promptly, enhancing the security posture of the application.

Option A is incorrect. While a penetration test can identify vulnerabilities in an application, it does not offer continuous monitoring or detection capabilities for ongoing malicious activities.

Option B is incorrect. While a firewall can provide a layer of security by filtering malicious traffic, it doesn't offer the granular insights or real-time monitoring needed to detect all unauthorized activities within an application.

Option D is incorrect. Training users about secure browsing habits is important but would not directly help in monitoring or detecting malicious activities on the e-commerce application.

Question 214. Ella, a security analyst, is reviewing the logs of a web application and notices that an attacker attempted to use the following input in a login form: ' OR '1'='1' --. This input was used in an effort to manipulate the application's backend database. What type of injection attack is this an example of?

- (A) XML Injection
- (B) Command Injection
- (C) **SQL Injection**
- (D) LDAP Injection

Explanation 214. Correct Answer: C. SQL Injection. The input ' OR '1'='1' -- is a classic example of an SQL injection attack. Attackers use this technique to manipulate SQL queries in applications that do not properly validate user input, potentially allowing unauthorized access or data retrieval.

Option A is incorrect. XML Injection targets applications that parse XML input. The payload mentioned in the scenario is not related to XML structures.

Option B is incorrect. Command Injection is when an attacker attempts to execute arbitrary commands on a host operating system. The given input is not an OS command.

Option D is incorrect. LDAP Injection targets applications that construct LDAP statements based on user input. The given payload is not structured for LDAP queries.

Question 215. A medium-sized company has just deployed a new file server for the HR department. They want to ensure that only HR employees can view and edit HR-specific documents, while the IT department should only be able to perform system maintenance tasks. What should the company implement to achieve this requirement?

- (A) Install a firewall between the HR and IT departments
- (B) Implement an Access Control List (ACL) for the file server**
- (C) Enforce a strong password policy for the HR department
- (D) Enable full disk encryption on the file server

Explanation 215. Correct Answer: B. Implement an Access Control List (ACL) for the file server. Access Control Lists (ACLs) define who can access a resource and what they can do with it once accessed. By setting up an ACL for the file server, the company can precisely define the permissions for HR and IT departments, ensuring that only authorized users have the right level of access to the data.

Option A is incorrect. Installing a firewall would limit network traffic between departments but would not provide granular access control to files on the server.

Option C is incorrect. While a strong password policy is essential for security, it doesn't differentiate access between HR and IT or control what users can do once they access the server.

Option D is incorrect. Full disk encryption protects data at rest, but it does not provide differentiated access to specific files or directories based on user roles.

Question 216. A e-commerce website suddenly experiences a sharp increase in traffic, causing the website to become slow and occasionally inaccessible. The IT team observes that a large number of requests are originating from multiple IP addresses spread across various countries. What type of network attack is the e-commerce website likely experiencing?

- (A) Man-in-the-middle attack
- (B) DNS spoofing
- (C) **Distributed denial-of-service (DDoS) attack**
- (D) ARP poisoning

Explanation 216. Correct Answer: C. Distributed denial-of-service (DDoS) attack. In a DDoS attack, the attacker uses multiple systems, often compromised ones from different locations, to flood a target system with requests, making the target slow or inaccessible.

Option A is incorrect. A man-in-the-middle attack involves an attacker secretly intercepting and possibly altering the communication between two parties. It doesn't lead to website inaccessibility due to high traffic.

Option B is incorrect. DNS spoofing is when an attacker introduces corrupt DNS cache information to redirect traffic to a different IP address, usually under the attacker's control. It doesn't cause increased traffic from various countries.

Option D is incorrect. ARP poisoning is a technique by which an attacker sends fake ARP messages onto a local area network. This is usually used to link an attacker's MAC address with the IP address of another host, causing any traffic meant for that IP address to be sent to the attacker instead.

Question 217. A security auditor found that a website's login form returns detailed error messages like "Incorrect column name" or "Table not found." Which type of vulnerability could attackers potentially exploit using this information?

- (A) Brute Force Attack
- (B) **Structured Query Language injection (SQLi)**
- (C) Man-in-the-Middle Attack
- (D) Session Hijacking

Explanation 217. Correct Answer: B. Structured Query Language injection (SQLi). When websites provide detailed database error messages, it can give attackers clues about the database structure, making it easier for them to craft successful SQL injection attacks.

By returning detailed database error messages, the website inadvertently provides attackers with valuable insights into the database structure and potential points of vulnerability. This can be used to refine and enhance SQLi attacks, enabling attackers to potentially access, modify, or delete data.

Option A is incorrect. A Brute Force Attack involves trying many passwords or passphrases to guess the right one. Detailed error messages from a database are not typically used in brute force attacks.

Option C is incorrect. Man-in-the-Middle Attack intercepts and possibly alters the communication between two parties. Database error messages are not directly related to this type of attack.

Option D is incorrect. Session Hijacking involves taking over an active user session. Detailed database error messages don't play a direct role in this type of attack.

Question 218. An employee at a large corporation has recently installed an app on his company-issued mobile device from a website instead of the approved app store. The app claimed to help boost productivity, but soon after, sensitive data from the mobile device was found to be transmitted to an unknown

server. What mobile vulnerability was exploited?

- (A) Inadequate password policies
- (B) Open Wi-Fi connection
- (C) **Mobile device side loading**
- (D) Lack of mobile device encryption

Explanation 218. Correct Answer: C. Mobile device side loading. Side loading refers to the practice of installing apps on a mobile device from sources other than the approved app store. This can expose the device to apps that have not been vetted for security, leading to potential data compromise, as described in the scenario.

Option A is incorrect. While inadequate password policies can expose a device to unauthorized access, the scenario specifically mentions an app installed from an unapproved source, which points to side loading.

Option B is incorrect. An open Wi-Fi connection can expose mobile devices to threats, but the main issue described in the scenario revolves around the installation of an app from an unapproved source.

Option D is incorrect. While mobile device encryption is essential to protect data, the issue in the scenario is related to side loading, not the encryption status of the device.

Question 219. The IT department of XYZ Corp noticed that server logs are recording user login attempts during non-business hours, specifically between 2:00 AM and 3:00 AM, a time when no scheduled tasks or backups are set to run. Which

of the following is the MOST plausible explanation for this unusual activity?

- (A) The company's employees are working overtime
- (B) There might be a time zone misconfiguration on the server
- (C) **An unauthorized user is trying to gain access to the server**
- (D) The server is automatically installing security patches

Explanation 219. Correct Answer: C. An unauthorized user is trying to gain access to the server. Out-of-cycle logging that occurs during unusual hours, especially when no scheduled tasks are set, can be a significant indicator of malicious activity. In this scenario, the logging of user login attempts during non-business hours suggests an unauthorized user might be attempting access.

Option A is incorrect. While employees might occasionally work overtime, regular login attempts specifically between 2:00 AM and 3:00 AM are suspicious.

Option B is incorrect. A time zone misconfiguration might cause time discrepancies in logs, but it wouldn't result in repeated login attempts.

Option D is incorrect. Automatic security patch installations wouldn't result in user login attempts.

Question 220. An employee notices a stranger standing unusually close to her with an unfamiliar device while she uses her RFID badge to enter the office building. A few days later,

her colleague's badge suddenly stops working, even though it was not reported lost or damaged. What type of attack should the security team suspect?

- (A) Brute force attack on the access control system
- (B) **RFID cloning**
- (C) Tailgating
- (D) RFID jamming

Explanation 220. Correct Answer: B. RFID cloning. RFID cloning involves making an unauthorized copy of an RFID badge or tag by capturing its signal. The stranger standing unusually close with a device might have been capturing the RFID signal to clone it.

Option A is incorrect. While a brute force attack on an access control system involves trying multiple combinations to gain access, the scenario does not describe multiple access attempts or any involvement with the system itself.

Option C is incorrect. Tailgating involves following an authorized individual into a secure area without the proper credentials. The scenario describes a potential RFID capture, not someone following another person.

Option D is incorrect. RFID jamming would involve interfering with the RFID signal to prevent it from working, not copying the RFID details for unauthorized use.

CHAPTER 3

IMPLEMENTATION

Questions 221-310

Question 221. The networking team at SecureNet Corp. is setting up a new branch office. They want to ensure secure connectivity between the branch office and the main office. Which of the following would BEST provide this?

- (A) Establishing a clear line of sight for wireless antennas between the two locations
- (B) Implementing a Virtual Private Network (VPN) between the two sites
- (C) Increasing bandwidth on the public internet connection at both locations
- (D) Using multi-factor authentication for all user accounts in both locations

Question 222. A rapidly growing e-commerce company has recently experienced an increase in cross-site scripting (XSS) and SQL injection attacks. The company wants to deploy a solution that specifically protects against these threats at the application layer. Which type of firewall would be most appropriate?

- (A) Stateful Packet Inspection Firewall
- (B) Proxy Firewall

- (C) Network Layer Firewall
- (D) Web Application Firewall (WAF)

Question 223. SecureNet, a cybersecurity firm, is implementing an Intrusion Detection System (IDS) for its enterprise client. Where should the IDS be placed for optimal detection of malicious activities?

- (A) Before the perimeter firewall to capture all inbound traffic
- (B) Between the perimeter firewall and the internal network to monitor the filtered traffic
- (C) Inside the DMZ to monitor only external service requests
- (D) Adjacent to each workstation for personalized security

Question 224. An online gaming platform experiences latency issues during multiplayer sessions, affecting the gameplay experience of its users. The company wants to ensure real-time responsiveness for its players worldwide. Which of the following solutions would BEST mitigate these latency issues?

- (A) Implementing a Content Delivery Network (CDN)
- (B) Introducing stricter user authentication methods
- (C) Deploying a centralized database server
- (D) Reducing the game's graphical fidelity

Question 225. The software development team at ABC Corp. has created a unique application that utilizes innovative algorithms. The company wants to ensure that competitors cannot legally copy or replicate their application's functionality. Which of the following would be the MOST suitable method to protect this intellectual property?

- (A) Copyright the user interface design
- (B) Apply for a patent for the innovative algorithms
- (C) Store the application code in an encrypted vault
- (D) Ensure all users sign an acceptable use policy (AUP)

Question 226. A company is evaluating its data storage options. They need a solution that provides them with the highest level of control over their hardware, software, and network configurations, allowing for customized security controls and measures. Which deployment model would best suit their needs?

- (A) Cloud-based Infrastructure
- (B) Hybrid Infrastructure
- (C) On-premises Infrastructure
- (D) Community Cloud

Question 227. An organization is evaluating different security solutions for their new branch office. They want to ensure that the chosen solution can be rapidly deployed with minimal configuration. Which of the following options BEST fulfills this requirement?

- (A) A customized Intrusion Prevention System (IPS) tailored to the organization's unique needs
- (B) A zero-touch provisioning firewall
- (C) An open-source firewall with extensive manual settings
- (D) A security information and event management (SIEM) solution requiring manual log source integration

Question 228. In a microservices architecture, each service should be designed with a specific principle to ensure it performs a specific task and interacts with other services

through well-defined interfaces. What principle is this referring to?

- (A) Principle of Least Privilege
- (B) Single Responsibility Principle
- (C) Open-Closed Principle
- (D) Zero Trust Model

Question 229. An organization that processes classified information is implementing a network infrastructure to ensure the highest level of data security. The CISO recommends using a network configuration that ensures the system remains completely disconnected from unsecured networks and any external connections. Which of the following describes this type of configuration?

- (A) DMZ (Demilitarized Zone)
- (B) VPN (Virtual Private Network)
- (C) VLAN (Virtual Local Area Network)
- (D) Air-gapped network

Question 230. A large financial institution is planning to upgrade its IT infrastructure to allow for a more efficient use of hardware resources, faster deployment of applications, and reduced server provisioning times. While evaluating different technologies, which of the following would directly address these needs?

- (A) Network Segmentation
- (B) Intrusion Detection System
- (C) Virtualization
- (D) Multi-Factor Authentication

Question 231. A financial institution wants to enhance the security of its wired network. The goal is to ensure that only authorized devices can connect to the network, and the authentication process should be based on credentials or digital certificates. Which of the following protocols would best serve this purpose?

- (A) SNMPv3
- (B) SSL/TLS
- (C) 802.1X EAP
- (D) DHCP

Question 232. TechBlitz Inc. recently underwent an IT audit, and one of the suggestions was to reduce the attack surface. Which of the following measures would be MOST effective in accomplishing this?

- (A) Increasing the password length requirement for all users
- (B) Implementing regular vulnerability assessments
- (C) Deactivating unused services and ports on servers
- (D) Implementing a strict BYOD (Bring Your Own Device) policy

Question 233. SafeMed, a medical facility, uses a life-saving medical device with embedded software. Recently, a security vulnerability was found in the software, but due to the device's FDA regulatory status and the software's design, it cannot be patched immediately. How should SafeMed address the security concerns related to this device?

- (A) Disconnect the device from all networks and only use it in standalone mode
- (B) Inform patients about the vulnerability and let them decide whether to use the device

- (C) Implement network segmentation and strictly control access to the device
- (D) Return the device to the manufacturer for a full refund

Question 234. A smart city project is deploying various IoT sensors across the city to gather data on traffic patterns, weather, pollution levels, and more. Which of the following is the MOST critical security consideration when deploying these sensors?

- (A) Ensuring high data transfer speeds to cater to the volume of data from the IoT sensors
- (B) Limiting the IoT devices to communicate only with specific, pre-defined servers
- (C) Installing physical locks on IoT devices to prevent theft
- (D) Allowing IoT devices to connect to any available network for data redundancy

Question 235. A multinational corporation is looking to replace its current firewalls at all its global branches. The IT director wants a solution that can perform stateful inspection of packets, application-level filtering, and integrate threat intelligence feeds for updated threat awareness. Which of the following would be the most suitable solution?

- (A) Stateful Packet Inspection Firewall
- (B) Proxy Server
- (C) Web Application Firewall (WAF)
- (D) Next-Generation Firewall (NGFW)

Question 236. A multinational organization with multiple branch offices is looking to simplify their WAN connectivity and reduce costs while ensuring that their inter-office data

transfers remain secure. Which technology would best fit their needs?

- (A) VLAN
- (B) MPLS
- (C) SD-WAN
- (D) DMZ

Question 237. A financial company wants to improve its web browsing security by intercepting and inspecting web traffic to prevent users from accessing malicious sites or downloading malware. They are looking for a solution that can act as an intermediary for requests from clients seeking resources from other servers. What should the company implement?

- (A) Network IDS
- (B) VPN Concentrator
- (C) Proxy server
- (D) Jump server

Question 238. In an IaaS (Infrastructure as a Service) model, which of the following tasks is typically the responsibility of the cloud customer in a standard Cloud Responsibility Matrix?

- (A) Physical security of data centers
- (B) Patching of host operating systems
- (C) Network infrastructure maintenance
- (D) Patching of guest operating systems

Question 239. In a cloud environment, which of the following matrices defines the shared responsibilities between the cloud provider and the customer for specific cloud service models?

- (A) Shared Accountability Matrix
- (B) Cloud Resource Allocation Table

- (C) Cloud Security Posture Matrix
- (D) Cloud Responsibility Matrix

Question 240. A financial organization collects and stores personally identifiable information (PII) of its customers. The company operates within jurisdictions that have strict regulations concerning the storage, transmission, and processing of such data. Which of the following strategies would be MOST appropriate for the company to ensure compliance with these regulations?

- (A) Use open source encryption algorithms without validation
- (B) Only store customer data in physical, on-site servers
- (C) Implement data classification and labeling procedures
- (D) Limit the number of administrators with access to the data

Question 241. During an annual review, a company discovered that one of its critical systems had several unscheduled downtimes over the year. The CTO has recommended a move towards high availability architecture to address this. What is the PRIMARY concern when implementing high availability?

- (A) Ensuring that there are no single points of failure
- (B) Ensuring that the system is patched regularly
- (C) Implementing multi-factor authentication
- (D) Storing backups in multiple geographical locations

Question 242. After a recent service outage, a hospital's IT team is reviewing the availability of its patient record system. They want to ensure the system remains operational, even in the event of hardware failures. Which of the following

considerations is MOST relevant to this requirement?

- (A) Implementing database mirroring
- (B) Regularly updating the system's antivirus definitions
- (C) Using strong encryption for data at rest
- (D) Conducting penetration testing on the system

Question 243. An enterprise wants to configure its firewall so that if a malfunction occurs, the firewall should automatically allow traffic to ensure business continuity. Which failure mode should be implemented?

- (A) Fail-safe
- (B) Fail-over
- (C) Fail-closed
- (D) Fail-open

Question 244. An organization with a single physical network infrastructure wants to separate the traffic of its finance department from that of the HR department. They do not want to set up entirely new physical networks but want to ensure that data packets from one department do not mix with the other's. What should the organization implement?

- (A) Air-gapped network
- (B) DMZ (Demilitarized Zone)
- (C) VLAN (Virtual Local Area Network)
- (D) VPN (Virtual Private Network)

Question 245. A large organization is considering deploying a solution that will allow employees to securely access company resources remotely using their personal devices. The organization wants a solution that can provide strong authentication and ensure that the data remains confidential

during transit. Which technology should be adopted?

- (A) Kerberos
- (B) Remote Desktop Services (RDS)
- (C) Remote Access VPN
- (D) SNMP

Question 246. An e-commerce company wants to ensure that their customers' credit card data remains confidential while in transit over the internet. They are seeking a protocol that can help in securing their website's communication. Which protocol would best fit this requirement?

- (A) IPSec
- (B) SSH
- (C) TLS
- (D) ICMP

Question 247. A rapidly growing e-commerce platform has been facing intermittent downtimes, especially during sale events. To ensure high availability and even distribution of traffic among servers, the company is considering deploying a specific type of network appliance. Which of the following should the company deploy?

- (A) Intrusion Detection System (IDS)
- (B) VPN concentrator
- (C) Load balancer
- (D) Proxy server

Question 248. An organization is transitioning its IT infrastructure to be cloud-centric and aims to adopt a zero-trust network approach. They are looking for a solution that integrates cloud security, zero-trust access, and WAN

capabilities, ensuring employees have consistent secure access regardless of their location. Which of the following best addresses their needs?

- (A) Remote Desktop Services (RDS)
- (B) Secure access service edge (SASE)
- (C) Content Delivery Network (CDN)
- (D) Virtual Local Area Network (VLAN)

Question 249. A medium-sized e-commerce company recently experienced a data breach due to an external attack. Post-incident analysis revealed that while there were indications of the attack in their network traffic, no alarms were raised at the time of the attack. The company now wants to implement a solution to actively monitor and take action against malicious network traffic. Which of the following should they deploy?

- (A) Intrusion Detection System (IDS)
- (B) Network Access Control (NAC)
- (C) Proxy server
- (D) Intrusion Prevention System (IPS)

Question 250. GreenTech, a data center company, is planning to expand its operations in a region known for frequent power outages. To maintain security posture and ensure continuity of operations, which of the following should be their PRIMARY consideration regarding power?

- (A) Using power-efficient servers to reduce electricity costs
- (B) Setting up solar panels to promote green energy
- (C) Investing in redundant power supplies and uninterruptible power systems (UPS)
- (D) Running operations only during peak daylight hours to ensure natural lighting

Question 251. A startup company anticipates rapid growth in its user base over the next year. They are considering an architectural model for their application that can handle the projected growth without performance issues. Which of the following would be the BEST design consideration for this situation?

- (A) Implementing strict password policies
- (B) Using a monolithic application design
- (C) Integrating a DDoS protection mechanism
- (D) Adopting a microservices architecture

Question 252. A healthcare provider is updating its network infrastructure. Due to the sensitive nature of the medical data they handle, they want to ensure that any anomalies or malicious activities in the network are immediately detected and alerted. Which system should they primarily consider?

- (A) Intrusion Prevention System (IPS)
- (B) Intrusion Detection System (IDS)
- (C) DHCP server
- (D) VPN concentrator

Question 253. The IT security team at a large corporation is evaluating monitoring tools for network traffic. They need a solution that can inspect network packets without introducing any potential latency or altering the network flow. Which type of device attribute should they consider?

- (A) Active IDS
- (B) Passive firewall
- (C) Active firewall
- (D) Passive IDS

Question 254. A developer at your company is excited about the scalability benefits of serverless architecture and has deployed a new service using it. However, you notice an increased bill due to the service even when it's not in use. Which of the following could be a contributing factor?

- (A) The serverless functions are continuously triggered by unintended events
- (B) The server hardware is outdated
- (C) The load balancer is misconfigured
- (D) The organization lacks a Content Delivery Network (CDN)

Question 255. After a recent security breach, CyberCorp is reviewing its software vendors for their responsiveness to vulnerabilities. Which of the following metrics would BEST assist CyberCorp in determining the timeliness and efficiency of security patches from a vendor?

- (A) The frequency of software updates released by the vendor
- (B) The vendor's quarterly financial reports
- (C) Time between vulnerability disclosure and patch release by the vendor
- (D) The number of features added by the vendor in the last software update

Question 256. XYZ Corp. has recently developed a new manufacturing process that reduces production costs by 50%. This process is not yet patented and is considered a trade secret. The company wants to ensure that employees do not disclose this process to competitors. Which of the following would be the MOST effective strategy to achieve this?

- (A) Providing employees with a bonus for keeping the process confidential
- (B) Conducting random checks of employee communications
- (C) Implementing a mandatory non-disclosure agreement (NDA) for all employees
- (D) Hosting quarterly seminars to educate employees about the value of the trade secret

Question 257. A large e-commerce platform is facing challenges during peak sale periods, where the influx of users causes slowdowns and occasional outages. Which of the following solutions would BEST improve scalability during these high-demand times?

- (A) Implement a centralized logging system
- (B) Employ auto-scaling cloud solutions
- (C) Increase the frequency of data backups
- (D) Mandate regular security training for employees

Question 258. An e-commerce company is preparing for an upcoming Black Friday sale, expecting a surge in web traffic. To ensure their systems remain responsive during the sale, which of the following would be the MOST effective strategy to implement?

- (A) Increasing password complexity for all users
- (B) Limiting the number of products on sale
- (C) Implementing a content delivery network (CDN)
- (D) Conducting a yearly security audit

Question 259. A multinational corporation has data centers located in different countries. Due to regulatory constraints,

remote access to these data centers is highly restricted. The company's IT administrators need a centralized way to access all data centers securely without directly accessing them from their workstations. Which solution should the company consider?

- (A) Setting up a DMZ
- (B) Implementing a Jump server
- (C) Deploying an Active Directory
- (D) Using a local Proxy

Question 260. Acme Corp is restructuring its internal network to improve its security posture. They aim to separate areas with different levels of trust. Which of the following approaches would BEST achieve this objective?

- (A) Implementing VLANs based on organizational departments
- (B) Setting up a perimeter firewall to segment external and internal traffic
- (C) Designing network zones based on data sensitivity and access requirements
- (D) Using a single, flat network for simplicity

Question 261. Your organization is implementing Infrastructure as Code (IaC) to deploy and manage its cloud infrastructure. As part of a security review, what is a primary concern regarding the use of IaC scripts?

- (A) Lack of graphical interface for infrastructure visualization
- (B) Hardcoding sensitive data within the scripts
- (C) Inability to scale the infrastructure dynamically
- (D) Incompatibility with non-cloud environments

Question 262. A cloud-based SaaS company wants to ensure its infrastructure can handle a potential influx of a large number of users in the future. Which of the following approaches would BEST meet this scalability consideration?

- (A) Implement a horizontal scaling strategy
- (B) Introduce multi-factor authentication
- (C) Deploy deep packet inspection tools
- (D) Implement a centralized logging system

Question 263. A software development company is looking to migrate its legacy applications to a more modern infrastructure. They want to ensure the applications can be deployed consistently across multiple environments without the challenges of varying dependencies and configurations. Which approach would best achieve this goal?

- (A) Virtual Machine Deployment
- (B) Bare-Metal Deployment
- (C) Containerization
- (D) Serverless Computing

Question 264. A large enterprise is considering a transition to a more flexible and programmable network architecture. They want to centralize the control plane, allowing for automated, programmable network configurations and rapid provisioning. Which network architecture model should they consider?

- (A) VLAN (Virtual Local Area Network)
- (B) MPLS (Multiprotocol Label Switching)
- (C) VPN (Virtual Private Network)
- (D) SDN (Software-Defined Networking)

Question 265. A global corporation has undergone several IT incidents in the past year, including outages due to natural disasters and cyber attacks. The CEO wants to ensure the organization's IT infrastructure can withstand or rapidly recover from disruptive events. Which of the following best encapsulates this requirement?

- (A) Adopting a Zero Trust Architecture
- (B) Implementing a strict password policy
- (C) Establishing a Business Continuity Plan (BCP) with emphasis on resilience
- (D) Regularly updating firewall rules

Question 266. A medical company has recently deployed a device to monitor patient heart rates in real time. This device uses a real-time operating system (RTOS) to guarantee immediate response times. The security team is concerned about potential risks. Which of the following would be a KEY recommendation to enhance the security of such devices?

- (A) Ensure real-time data analysis capabilities
- (B) Integrate the device with the corporate cloud for backups
- (C) Implement strict network segmentation for the device
- (D) Increase the storage capacity of the device

Question 267. A small business wants to deploy a single network security device that can handle multiple security functions such as firewall protection, intrusion detection, anti-malware, and content filtering. Which of the following would be the most suitable solution?

- (A) Network Intrusion Detection System (NIDS)
- (B) Web Application Firewall (WAF)

- (C) Unified Threat Management (UTM)
- (D) Proxy Server

Question 268. An e-commerce company is experiencing attacks that specifically target the shopping cart feature of its web application. They want to implement a firewall that can understand web application-specific commands and provide protection. Which type of firewall should they consider?

- (A) Layer 4 Firewall
- (B) Layer 2 Firewall
- (C) Layer 7 Firewall
- (D) Packet Filtering Firewall

Question 269. A financial organization's high-security data center has an authentication system for its main entry. If the system encounters an unexpected error, the organization wants to ensure that no one can gain access to the data center until the system is fixed. Which configuration should the authentication system be set to?

- (A) Fail-open
- (B) Fail-closed
- (C) Fail-secure
- (D) Fail-passive

Question 270. A multinational company wants to allow its remote employees to securely access the corporate intranet over the Internet. The company's primary concern is to ensure data confidentiality and integrity during transit. Which solution should the company implement?

- (A) VLAN
- (B) VPN

- (C) NAC
- (D) DMZ

Question 271. After conducting a business impact analysis, a local library determined that they could afford several days of downtime without a significant impact on their operations. They want a disaster recovery solution that offers a balance between cost and recovery capabilities. Which site consideration is the most suitable for the library's needs?

- (A) Mobile site with a full set of IT equipment
- (B) Hot site with daily data replication
- (C) Cold site
- (D) Warm site with weekly backups

Question 272. An online payment gateway is evaluating methods to enhance the security of its payment processing system. They want a solution that replaces sensitive cardholder data with a unique identifier that has no intrinsic value by itself. Which method should they implement?

- (A) Hashing the card data
- (B) Encrypting the card data
- (C) Masking the card data
- (D) Tokenizing the card data

Question 273. A software company is developing a new cloud-based application where clients can store and manage their customer contact details. The stored data does not include financial or medical information but does contain phone numbers and email addresses. How should this information be classified?

- (A) Public

- (B) Restricted
- (C) Sensitive
- (D) Classified

Question 274. Cybertech Corp. is reviewing its backup protocols to enhance security. They decided that before transferring backups to an offsite location, the data should be rendered unreadable to unauthorized individuals. Which backup strategy will ensure this requirement is met?

- (A) Use deduplication before storing backups
- (B) Store backups in proprietary formats
- (C) Encrypt backups before transfer
- (D) Compress backups using standard tools

Question 275. After a major power outage, TechWave Corp. wants to ensure their primary data center's operations can be swiftly and seamlessly shifted to another facility. The company wants this process to be automated and immediate to prevent any service interruption. What type of test should TechWave Corp. conduct to validate this functionality?

- (A) Conduct a vulnerability assessment on both data centers
- (B) Execute a failover test
- (C) Engage in a tabletop exercise
- (D) Perform a routine backup test

Question 276. A pharmaceutical company is working on a new drug formula that promises to revolutionize the treatment of a particular disease. The R&D team has detailed documentation on the components, procedures, and results of the drug trials. How should this documentation be classified to ensure that only the right people within the company have access?

- (A) Unclassified
- (B) Public
- (C) Confidential
- (D) Sensitive

Question 277. A software development company maintains a shared code repository. The company wants to ensure that only developers can make changes to the code, but testers should be able to view the code without modifying it. Which approach should be implemented?

- (A) Assign all employees read-only permissions
- (B) Provide testers with administrative rights
- (C) Implement role-based access controls (RBAC)
- (D) Use data encryption on the repository

Question 278. A software development company has just expanded its team and wants to ensure that in the event of a disaster, they can resume operations within a day. However, they have a limited budget for disaster recovery. Which of the following disaster recovery site types would be the most suitable for the company's needs?

- (A) Hot site with hourly data replication
- (B) Cold site with monthly data backups
- (C) Warm site with daily backups
- (D) Offsite tape backups

Question 279. A financial institution wants to ensure that if a cyber attacker gains unauthorized access to one section of their network, the attacker cannot easily move laterally to more sensitive parts of the network. Which method can help achieve this objective?

- (A) Deploying a honeypot in every segment
- (B) Implementing network segmentation
- (C) Applying encryption on all data traffic
- (D) Enabling two-factor authentication for all users

Question 280. DataFin, a financial analytics firm, experienced a minor fire incident in one of its server rooms. Fortunately, they had backups stored in another wing of the building, allowing for quick data recovery. However, management realizes that in a major disaster, both primary and backup data might be destroyed. To address this, which backup strategy should DataFin consider?

- (A) Mirror Backup
- (B) Local Storage Backup
- (C) Incremental Backup
- (D) Offsite Backup

Question 281. A healthcare organization with patients worldwide is planning to set up a backup site for its medical data repository. They have been advised to consider geographic dispersion as part of their disaster recovery plan. Which of the following reasons is the LEAST valid for geographic dispersion in this scenario?

- (A) Mitigate risks of regional natural disasters
- (B) Offer redundancy in case of local power outages
- (C) Benefit from varying peak load times in different regions
- (D) Ensure faster access speeds for global patients

Question 282. A multinational corporation is expanding its operations in various countries. The company has decided to

restrict access to its internal network based on geolocation to ensure that only employees from specific countries can access certain data. Which of the following would be the MOST appropriate solution to implement this requirement?

- (A) Deploy a VPN with multi-factor authentication
- (B) Use MAC address filtering on all company devices
- (C) Implement a geolocation-based access control system
- (D) Set up region-specific SSIDs for the company's Wi-Fi network

Question 283. DigitalFront, an e-commerce company, is expecting a surge in traffic during their upcoming annual sale event. They want to ensure that their website and applications can handle the anticipated increase in user activity without any performance degradation. Which of the following steps is MOST relevant to achieving this goal?

- (A) Increasing the frequency of security audits
- (B) Implementing capacity planning specifically focused on technology
- (C) Adopting multi-factor authentication for all users
- (D) Investing in advanced threat intelligence solutions

Question 284. DeltaTech, a financial institution, operates its primary site on a UNIX-based platform. For disaster recovery purposes, they are considering setting up a backup site on a different platform. Which of the following is NOT a primary benefit of introducing platform diversity in this case?

- (A) It reduces the organization's learning curve by using familiar technologies
- (B) It provides resilience against attacks targeting UNIX-based systems

- (C) It ensures that platform-specific outages don't affect both primary and backup sites
- (D) It diversifies the attack surface, reducing the impact of specific platform vulnerabilities

Question 285. After a recent system upgrade, CloudTech Corp. decided to validate the efficiency and reliability of its new data processing system. To do this, they run the new system alongside the old one and compare the outcomes. This way, they aim to ensure that the new system is both robust and capable of handling the current workload. What kind of testing is CloudTech Corp. utilizing?

- (A) Load Testing
- (B) Failover Testing
- (C) Parallel Processing Testing
- (D) Simulation Testing

Question 286. TechSolutions Inc., a rapidly growing startup, is expanding its workforce to meet its customer demands. As part of this expansion, they need to ensure their IT infrastructure can accommodate the influx of new employees without compromising performance or security. Which of the following should be TechSolutions' primary focus during this expansion phase?

- (A) Adopting a Zero Trust Network Architecture
- (B) Increasing the frequency of vulnerability assessments
- (C) Implementing capacity planning
- (D) Deploying additional firewalls and intrusion detection systems

Question 287. StreamNet, a popular online streaming service, is planning to launch in three new countries. They anticipate a substantial increase in users and concurrent streams. To ensure that the service remains uninterrupted and provides a seamless experience to new users, which action related to capacity planning should StreamNet prioritize?

- (A) Investing in content encryption and DRM
- (B) Increasing marketing and promotional activities in the new countries
- (C) Implementing stronger user authentication methods
- (D) Expanding and optimizing their infrastructure to handle the projected growth

Question 288. GlobalTech is implementing a disaster recovery plan and wants to ensure continuous availability with no data loss. They have decided to use replication as a backup strategy. Which of the following replication techniques should GlobalTech implement to achieve their objective?

- (A) Periodic replication scheduled daily
- (B) Asynchronous replication with hourly synchronization
- (C) Synchronous replication
- (D) Snapshot replication every 30 minutes

Question 289. A software company has developed a new product. They want to release a user manual that details how to use the software, its features, and basic troubleshooting steps. What should be the classification of this user manual?

- (A) Confidential
- (B) Restricted
- (C) Public
- (D) Internal

Question 290. A global finance firm has recently faced downtime due to unexpected disasters in its main operational region. The firm wishes to have a backup site that would allow them to continue their operations with minimal downtime and no data loss. Which type of backup site would be the most appropriate for the firm?

- (A) Cold site
- (B) Warm site
- (C) Hot site
- (D) Mobile site

Question 291. An international bank is setting up a new online portal for its customers to access their financial statements. Which measure should the bank implement to ensure that financial data in transit between the customer's browser and the bank's servers is kept confidential?

- (A) Use file-level encryption for all financial statements
- (B) Implement a Web Application Firewall (WAF)
- (C) Use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for the portal
- (D) Store all financial data in an encrypted database

Question 292. A global e-commerce website wants to allow its customer service representatives to assist clients with order issues without exposing the full credit card details of the clients. Which method should the IT department employ to achieve this?

- (A) Replace all digits of the credit card number with random characters
- (B) Display only the last four digits of the credit card number while masking the rest

- (C) Encrypt the credit card number with a symmetric key
- (D) Use a hash function to represent the credit card number

Question 293. XYZ Corp recently faced a ransomware attack that encrypted critical data files. The company's IT team was unable to decrypt the files but had a recent backup available. However, when they tried to restore the data, they found out the backup was corrupted. Which of the following best practices would have helped XYZ Corp in ensuring the integrity of their backups?

- (A) Regularly testing backup restoration processes
- (B) Storing backups in the same directory as original files
- (C) Increasing the frequency of backups to every hour
- (D) Encrypting backups with a strong encryption algorithm

Question 294. A financial institution is updating its infrastructure to ensure that customer financial data is kept secure from both internal and external threats. Which of the following would be the MOST effective measure to protect customer financial data from being accessed by unauthorized internal users?

- (A) Deploying perimeter firewalls around the institution's network
- (B) Implementing two-factor authentication (2FA) for all customer accounts
- (C) Enforcing strict access controls based on the principle of least privilege
- (D) Conducting yearly cybersecurity awareness training for all employees

Question 295. A company's proprietary algorithm is being targeted by competitors aiming to replicate its functionality. To safeguard its intellectual property without changing the algorithm's behavior, the company wants a method that disguises the original code structure. What should they implement?

- (A) Data masking on the algorithm's output
- (B) Obfuscation on the algorithm's code
- (C) Encryption of the algorithm's storage location
- (D) Implementing a hashing mechanism within the algorithm

Question 296. A multinational e-commerce company is expanding its infrastructure to handle increasing traffic. The primary goal is to distribute the incoming web traffic across multiple servers to ensure that no single server is overwhelmed. Which method should the company use?

- (A) Deploy a web application firewall
- (B) Implement server clustering
- (C) Use hardware-based firewalls
- (D) Set up a load balancer

Question 297. A law firm is transitioning to a digital storage system and wants to ensure that client records and case files are protected from unauthorized access. Which of the following would be the BEST strategy to ensure the confidentiality of legal information stored digitally?

- (A) Conducting regular penetration testing on the digital storage system
- (B) Encrypting the client records and case files

- (C) Applying watermarks to digital documents
- (D) Limiting physical access to the server room

Question 298. A healthcare provider stores vast amounts of patient data on its servers. While they have strong perimeter defenses, they want an additional layer of security to ensure patient data remains confidential even in the event of unauthorized access. Which of the following would be the MOST effective solution for this requirement?

- (A) Use hash algorithms on all patient data
- (B) Implement data deduplication techniques
- (C) Encrypt the stored patient data
- (D) Use a web application firewall (WAF)

Question 299. After a major outage, CloudTech Services is reviewing their disaster recovery strategy. The company found out that after restoring from backup, several applications did not function properly due to configuration discrepancies. What would be the best approach to ensure a successful recovery in the future?

- (A) Prioritize applications for backup based on their importance
- (B) Implement differential backups in addition to full backups
- (C) Regularly conduct a full system recovery in a test environment
- (D) Use a third-party backup solution instead of an in-house solution

Question 300. A financial institution is implementing a system where customers can verify the integrity of their monthly

statements without having access to the original data. Which of the following techniques would be MOST appropriate for this task?

- (A) Encrypting the statements using AES
- (B) Compressing the statements to reduce file size
- (C) Hashing the statements and providing the hash value to the customers
- (D) Tokenizing sensitive data within the statements

Question 301. An organization has decided to focus on securing its database servers where customer details and transaction records are stored. This data is not being actively accessed or processed. Which type of security measure would be MOST appropriate for this type of data?

- (A) VLDData Loss Prevention (DLP) for emailAN
- (B) Web Application Firewall (WAF)
- (C) Full Disk Encryption (FDE)
- (D) Intrusion Detection System (IDS) for network traffic

Question 302. A multinational company is considering using a cloud storage provider based in a foreign country to store customer data. The company's home country has strict data protection laws that require customer data to remain within its borders. Which of the following considerations is MOST critical for the company when choosing the cloud storage provider?

- (A) The speed of data access from the foreign-based cloud storage
- (B) The encryption standards used by the foreign cloud provider
- (C) Whether the foreign cloud provider offers data storage

exclusively within the company's home country

(D) The reputation and customer reviews of the foreign cloud provider

Question 303. After an annual review, BestTech Co. realized that their IT team was unfamiliar with the protocols to follow during a data breach. To ensure the team understands the steps and decision points without launching a live drill, what should the company implement?

(A) Upgrade their firewall systems

(B) Engage in a tabletop exercise

(C) Conduct a red team exercise

(D) Implement multi-factor authentication for all users

Question 304. SecureData Inc., a financial firm, recently experienced a system crash and needed to restore their database. While they had a full backup from the previous week, they realized that several days of transactions were missing. To prevent such data loss in the future, which backup strategy involving recording transactions can SecureData implement?

(A) Implement differential backups

(B) Use snapshot backups every hour

(C) Enable database journaling

(D) Configure RAID 5 for their storage

Question 305. SecureNet Inc. recently upgraded their security infrastructure. To validate how the new system would respond in real-world scenarios without exposing it to actual risks, they decide to imitate certain cyber threats in a controlled environment. Which type of test is SecureNet Inc. planning to conduct?

- (A) Penetration Testing
- (B) Simulation Testing
- (C) Vulnerability Assessment
- (D) Failover Testing.

Question 306. ZenTech, a multinational corporation, recently adopted a multi-cloud strategy, deploying workloads across multiple cloud service providers. What is a primary security benefit of this approach?

- (A) Centralized management of all cloud resources
- (B) Automatic encryption of data in transit between clouds
- (C) Mitigation against a single point of failure
- (D) Reduction in the cost of cloud storage solutions

Question 307. GlobalBank has implemented a backup strategy where only the changes made since the last full backup are recorded. Considering the need to optimize storage and reduce backup times, the IT team performs this type of backup every day. What backup frequency and type is GlobalBank utilizing?

- (A) Incremental Backup daily
- (B) Differential Backup weekly
- (C) Full Backup bi-weekly
- (D) Snapshot Backup daily

Question 308. A defense contractor is working on a new missile system. While the detailed schematics and operational details are classified, they have an overview document that only a select group of partners and stakeholders can view. How should this overview document be classified?

- (A) Public
- (B) Restricted

- (C) Confidential
- (D) Top Secret

Question 309. A tech startup is developing a mobile application that offers exclusive content only to users within a specific country due to licensing agreements. Which method should the startup use to ensure that only users within that country can access the content?

- (A) Integrate a time-based one-time password (TOTP) system
- (B) Use geolocation-based access controls
- (C) Enable biometric authentication
- (D) Implement IP whitelisting

Question 310. MetroTech recently experienced an incident where an employee mistakenly deleted a portion of their database. The IT team was able to restore the data using a backup snapshot taken 24 hours prior. However, some data loss still occurred. Which of the following recommendations would minimize data loss in a similar situation in the future?

- (A) Configure backup snapshots to be taken on a weekly basis
- (B) Employ a differential backup solution in addition to snapshots
- (C) Increase the storage capacity for backups
- (D) Use an hourly snapshot backup schedule

Answers 221-310

Question 221. The networking team at SecureNet Corp. is setting up a new branch office. They want to ensure secure connectivity between the branch office and the main office. Which of the following would BEST provide this?

- (A) Establishing a clear line of sight for wireless antennas between the two locations
- (B) Implementing a Virtual Private Network (VPN) between the two sites**
- (C) Increasing bandwidth on the public internet connection at both locations
- (D) Using multi-factor authentication for all user accounts in both locations

Explanation 221. Correct Answer: B. Implementing a Virtual Private Network (VPN) between the two sites. VPNs provide secure, encrypted connections over potentially insecure networks, such as the internet, making them ideal for securely connecting remote locations.

Option A is incorrect. While a clear line of sight might facilitate wireless communication, it doesn't inherently provide secure connectivity.

Option C is incorrect. Increasing bandwidth enhances data transfer rates but doesn't inherently secure the connection between sites.

Option D is incorrect. Multi-factor authentication is a robust security measure for user access but doesn't secure network connectivity between sites.

Question 222. A rapidly growing e-commerce company has recently experienced an increase in cross-site scripting (XSS) and SQL injection attacks. The company wants to deploy a solution that specifically protects against these threats at the application layer. Which type of firewall would be most appropriate?

- (A) Stateful Packet Inspection Firewall
- (B) Proxy Firewall
- (C) Network Layer Firewall
- (D) **Web Application Firewall (WAF)**

Explanation 222. Correct Answer: D. Web Application Firewall (WAF). A Web Application Firewall (WAF) is specifically designed to protect web applications by monitoring, filtering, and blocking potentially harmful HTTP traffic. This includes protection against threats like XSS and SQL injection attacks that are common against web applications.

Option A is incorrect. While a Stateful Packet Inspection Firewall can monitor the state of active connections and make decisions based on the context of the traffic, it doesn't specifically address application layer vulnerabilities like XSS and SQL injection.

Option B is incorrect. Although a Proxy Firewall can provide some application layer filtering, its primary purpose is not

tailored to protect against specific web application vulnerabilities.

Option C is incorrect. A Network Layer Firewall primarily operates at the network layer and won't provide specialized protection against application layer threats.

Question 223. SecureNet, a cybersecurity firm, is implementing an Intrusion Detection System (IDS) for its enterprise client. Where should the IDS be placed for optimal detection of malicious activities?

- (A) Before the perimeter firewall to capture all inbound traffic
- (B) **Between the perimeter firewall and the internal network to monitor the filtered traffic**
- (C) Inside the DMZ to monitor only external service requests
- (D) Adjacent to each workstation for personalized security

Explanation 223. Correct Answer: B. Between the perimeter firewall and the internal network to monitor the filtered traffic. By placing the IDS between the firewall and the internal network, it can monitor traffic that has passed through the firewall's filters. This position provides a balance between capturing potential threats and reducing false positives from benign external traffic.

Option A is incorrect. While placing the IDS before the firewall will capture all inbound traffic, it may result in a high number of false positives since a lot of benign traffic might trigger alarms.

Option C is incorrect. Placing the IDS only in the DMZ would limit its visibility to only external service requests and not the overall internal traffic which might have potential threats.

Option D is incorrect. While personal IDS on each workstation provides granular monitoring, it does not provide a holistic view of network activities and can be resource-intensive.

Question 224. An online gaming platform experiences latency issues during multiplayer sessions, affecting the gameplay experience of its users. The company wants to ensure real-time responsiveness for its players worldwide. Which of the following solutions would BEST mitigate these latency issues?

- (A) **Implementing a Content Delivery Network (CDN)**
- (B) Introducing stricter user authentication methods
- (C) Deploying a centralized database server
- (D) Reducing the game's graphical fidelity

Explanation 224. Correct Answer: A. Implementing a Content Delivery Network (CDN). A CDN involves distributing the hosting of content to multiple locations around the world. For online gaming, this means players can connect to a server closer to their geographic location, thereby reducing latency and improving responsiveness.

Option B is incorrect. While strong authentication methods are crucial for security, they don't address latency or improve the real-time responsiveness of the gaming platform.

Option C is incorrect. Centralizing the database server might actually increase latency for users who are far from the central location.

Option D is incorrect. Reducing graphical fidelity can improve game performance on the client side, but it doesn't address network latency or the real-time responsiveness of multiplayer sessions.

Question 225. The software development team at ABC Corp. has created a unique application that utilizes innovative algorithms. The company wants to ensure that competitors cannot legally copy or replicate their application's functionality. Which of the following would be the MOST suitable method to protect this intellectual property?

- (A) Copyright the user interface design
- (B) **Apply for a patent for the innovative algorithms**
- (C) Store the application code in an encrypted vault
- (D) Ensure all users sign an acceptable use policy (AUP)

Explanation 225. Correct Answer: B. Apply for a patent for the innovative algorithms. Patents provide legal protection for inventions, allowing the inventor or patent holder the exclusive right to the patented process, design, or invention for a certain period. In this case, patenting the algorithms would prevent competitors from legally replicating the application's unique functionality.

Option A is incorrect. Copyrighting the user interface design would only protect the visual appearance and elements of the

application, not its unique functionality or underlying algorithms.

Option C is incorrect. While storing the application code in an encrypted vault protects it from unauthorized access, it does not provide legal protection against replication by competitors if they develop similar functionality independently.

Option D is incorrect. An acceptable use policy (AUP) defines how users are allowed to use the software or system, but it doesn't offer protection against competitors copying the application's unique functionality.

Question 226. A company is evaluating its data storage options. They need a solution that provides them with the highest level of control over their hardware, software, and network configurations, allowing for customized security controls and measures. Which deployment model would best suit their needs?

- (A) Cloud-based Infrastructure
- (B) Hybrid Infrastructure
- (C) **On-premises Infrastructure**
- (D) Community Cloud

Explanation 226. Correct Answer: C. On-premises Infrastructure. On-premises infrastructure allows organizations to have complete control over their hardware, software, and network configurations. This gives them the freedom to customize security controls and measures tailored to their specific needs.

Option A is incorrect. Cloud-based infrastructures are hosted by third-party providers, which means organizations might not have the same level of control or customization over their resources.

Option B is incorrect. Hybrid infrastructure combines on-premises and cloud resources. While it offers more control than purely cloud-based solutions, it still doesn't provide the total control that on-premises infrastructure does.

Option D is incorrect. A community cloud is shared by several organizations with similar requirements. While it offers some level of control, it doesn't provide the complete customization and control that an on-premises infrastructure does.

Question 227. An organization is evaluating different security solutions for their new branch office. They want to ensure that the chosen solution can be rapidly deployed with minimal configuration. Which of the following options BEST fulfills this requirement?

- (A) A customized Intrusion Prevention System (IPS) tailored to the organization's unique needs
- (B) A zero-touch provisioning firewall
- (C) An open-source firewall with extensive manual settings
- (D) A security information and event management (SIEM) solution requiring manual log source integration

Explanation 227. Correct Answer: B. A zero-touch provisioning firewall. Zero-touch provisioning allows devices to be provisioned and configured automatically, ensuring rapid deployment with minimal manual intervention.

Option A is incorrect. While a customized IPS might be tailored for the organization's needs, it often requires a lot of configuration and isn't the fastest to deploy.

Option C is incorrect. Open-source firewalls that require extensive manual settings are not considered rapid to deploy as they necessitate more time for configuration.

Option D is incorrect. A SIEM solution that requires manual log source integration would not be the quickest to deploy due to the manual steps involved.

Question 228. In a microservices architecture, each service should be designed with a specific principle to ensure it performs a specific task and interacts with other services through well-defined interfaces. What principle is this referring to?

- (A) Principle of Least Privilege
- (B) **Single Responsibility Principle**
- (C) Open-Closed Principle
- (D) Zero Trust Model

Explanation 228. Correct Answer: B. Single Responsibility Principle. The Single Responsibility Principle dictates that a class or module (or in the context of microservices, a service) should have only one reason to change, meaning it should only have one job or responsibility. In microservices, this ensures that each service does one thing and does it well, and interacts with others through clear interfaces.

Option A is incorrect. The Principle of Least Privilege is about ensuring that users or services have only the permissions they need to perform their tasks and nothing more. It's not specifically about the design of the service itself.

Option C is incorrect. The Open-Closed Principle is a design principle stating that software entities should be open for extension but closed for modification. While relevant for software design, it's not the primary principle guiding the design of individual microservices.

Option D is incorrect. The Zero Trust Model is a security concept where no one, whether inside or outside the organization, is trusted by default. It's not a principle specific to microservice design.

Question 229. An organization that processes classified information is implementing a network infrastructure to ensure the highest level of data security. The CISO recommends using a network configuration that ensures the system remains completely disconnected from unsecured networks and any external connections. Which of the following describes this type of configuration?

- (A) DMZ (Demilitarized Zone)
- (B) VPN (Virtual Private Network)
- (C) VLAN (Virtual Local Area Network)
- (D) **Air-gapped network**

Explanation 229. Correct Answer: D. Air-gapped network.

An air-gapped network is a network that is physically isolated from unsecured networks. Computers on an air-gapped network

cannot communicate with non-air-gapped computers and aren't connected to external networks or the internet, ensuring the highest level of data security.

Option A is incorrect. A DMZ is a buffer zone between a private network and external networks (typically the internet). It's designed to provide an additional layer of security but does not guarantee complete isolation.

Option B is incorrect. VPNs are used to establish secure connections over an unsecured network, such as the internet. They encrypt the data being transferred but don't physically isolate a network.

Option C is incorrect. A VLAN is a logically segmented network within a physical network. It allows for the separation of broadcast domains in a Layer 2 network, but it doesn't provide complete physical isolation from other networks.

Question 230. A large financial institution is planning to upgrade its IT infrastructure to allow for a more efficient use of hardware resources, faster deployment of applications, and reduced server provisioning times. While evaluating different technologies, which of the following would directly address these needs?

- (A) Network Segmentation
- (B) Intrusion Detection System
- (C) **Virtualization**
- (D) Multi-Factor Authentication

Explanation 230. Correct Answer: C. Virtualization.

Virtualization allows multiple virtual machines to run on a single physical host, maximizing the use of hardware resources. It enables rapid provisioning and deployment of new servers and applications, addressing the requirements of the financial institution.

Option A is incorrect. Network segmentation divides a network into smaller subnetworks, primarily for security and performance reasons. While it's a best practice, it doesn't address the efficient use of hardware or rapid deployment of applications.

Option B is incorrect. An Intrusion Detection System (IDS) monitors and detects malicious activities in a network. While crucial for security, it doesn't cater to hardware resource efficiency or faster server provisioning.

Option D is incorrect. Multi-Factor Authentication is a security process in which a user provides multiple methods of identification to authenticate their identity. It doesn't impact hardware resource efficiency or application deployment times.

Question 231. A financial institution wants to enhance the security of its wired network. The goal is to ensure that only authorized devices can connect to the network, and the authentication process should be based on credentials or digital certificates. Which of the following protocols would best serve this purpose?

- (A) SNMPv3
- (B) SSL/TLS

- (C) 802.1X EAP
- (D) DHCP

Explanation 231. Correct Answer: C. 802.1X EAP. 802.1X Extensible Authentication Protocol (EAP) provides port-based network access control and is used on wired networks to ensure that only authenticated devices can connect. It supports multiple authentication methods including credentials, digital certificates, and smart cards.

Option A is incorrect. SNMPv3 (Simple Network Management Protocol version 3) is used for network management and monitoring, not for port-based network access control.

Option B is incorrect. SSL/TLS (Secure Sockets Layer/Transport Layer Security) is a protocol used for securing data transmission on the internet, not for port-based network access control.

Option D is incorrect. DHCP (Dynamic Host Configuration Protocol) assigns IP addresses to devices on a network but doesn't deal with port-based authentication.

Question 232. TechBlitz Inc. recently underwent an IT audit, and one of the suggestions was to reduce the attack surface. Which of the following measures would be MOST effective in accomplishing this?

- (A) Increasing the password length requirement for all users
- (B) Implementing regular vulnerability assessments
- (C) **Deactivating unused services and ports on servers**

(D) Implementing a strict BYOD (Bring Your Own Device) policy

Explanation 232. Correct Answer: C. Deactivating unused services and ports on servers. Reducing the number of active services and ports directly diminishes the number of potential entry points for attackers, thus reducing the attack surface.

Option A is incorrect. While increasing password length improves security against brute-force attacks, it doesn't directly affect the attack surface.

Option B is incorrect. Regular vulnerability assessments identify potential security gaps, but simply identifying doesn't reduce the attack surface unless actions are taken based on findings.

Option D is incorrect. A strict BYOD policy can enhance security, but it's focused more on the types of devices and how they connect rather than reducing the number of potential attack points.

Question 233. SafeMed, a medical facility, uses a life-saving medical device with embedded software. Recently, a security vulnerability was found in the software, but due to the device's FDA regulatory status and the software's design, it cannot be patched immediately. How should SafeMed address the security concerns related to this device?

(A) Disconnect the device from all networks and only use it in standalone mode

(B) Inform patients about the vulnerability and let them

decide whether to use the device

(C) Implement network segmentation and strictly control access to the device

(D) Return the device to the manufacturer for a full refund

Explanation 233. Correct Answer: C. Implement network segmentation and strictly control access to the device. By implementing network segmentation, SafeMed can isolate the vulnerable device from other parts of the network, reducing the risk of potential exploitation. Strictly controlling access ensures only authorized personnel can use or interact with the device.

Option A is incorrect. Completely disconnecting the device might limit its functionality, especially if it needs network access for updates, data transfer, or other essential operations.

Option B is incorrect. While transparency is important, simply informing patients without taking protective measures may not be enough to ensure safety and could lead to panic or misinformation.

Option D is incorrect. Returning the device might not be feasible, especially if there are no immediate replacements available, and it is vital for patient care.

Question 234. A smart city project is deploying various IoT sensors across the city to gather data on traffic patterns, weather, pollution levels, and more. Which of the following is the MOST critical security consideration when deploying these sensors?

(A) Ensuring high data transfer speeds to cater to the

volume of data from the IoT sensors

(B) Limiting the IoT devices to communicate only with specific, pre-defined servers

(C) Installing physical locks on IoT devices to prevent theft

(D) Allowing IoT devices to connect to any available network for data redundancy

Explanation 234. Correct Answer: B. Limiting the IoT devices to communicate only with specific, pre-defined servers. By restricting IoT devices to communicate only with specific, trusted servers, unauthorized access and data tampering risks can be minimized. This measure ensures that data is only sent to and received from legitimate sources.

Option A is incorrect. While data transfer speeds are important for performance and real-time analytics, from a security standpoint, the integrity and confidentiality of the data is more crucial.

Option C is incorrect. While physical security is an essential aspect, especially in a public setting, the most significant risks with IoT often pertain to data security and unauthorized access.

Option D is incorrect. Allowing IoT devices to connect to any available network can introduce significant security vulnerabilities, such as man-in-the-middle attacks, eavesdropping, or unauthorized data tampering.

Question 235. A multinational corporation is looking to replace its current firewalls at all its global branches. The IT director wants a solution that can perform stateful inspection of packets,

application-level filtering, and integrate threat intelligence feeds for updated threat awareness. Which of the following would be the most suitable solution?

- (A) Stateful Packet Inspection Firewall
- (B) Proxy Server
- (C) Web Application Firewall (WAF)
- (D) **Next-Generation Firewall (NGFW)**

Explanation 235. Correct Answer: D. Next-Generation Firewall (NGFW). Next-Generation Firewalls (NGFWs) are designed to offer traditional firewall capabilities such as stateful inspection but also come with advanced features like application-level filtering and the ability to integrate with threat intelligence feeds. This makes NGFWs suitable for modern, complex environments that demand multi-layered security features.

Option A is incorrect. While a Stateful Packet Inspection Firewall can monitor the state of active connections and analyze the packets, it doesn't offer advanced features like application-level filtering or the integration of threat intelligence feeds that a NGFW does.

Option B is incorrect. A Proxy Server controls and filters requests from clients to servers, typically for web access. It doesn't possess the comprehensive security functionalities of a NGFW.

Option C is incorrect. A Web Application Firewall (WAF) specifically protects web applications from targeted attacks.

While valuable, it doesn't offer the breadth of features and integrations that a NGFW does.

Question 236. A multinational organization with multiple branch offices is looking to simplify their WAN connectivity and reduce costs while ensuring that their inter-office data transfers remain secure. Which technology would best fit their needs?

- (A) VLAN
- (B) MPLS
- (C) **SD-WAN**
- (D) DMZ

Explanation 236. Correct Answer: C. SD-WAN. Software-defined wide area network (SD-WAN) offers enterprises the ability to leverage any combination of transport services, including MPLS, LTE, and broadband internet services, to securely connect users to applications. SD-WAN can reduce costs by enabling the use of lower-cost internet connections and can also simplify WAN management.

Option A is incorrect. VLAN (Virtual Local Area Network) is used to segment a local network into different broadcast domains, but it does not facilitate WAN connectivity or reduce WAN costs.

Option B is incorrect. MPLS (Multi-Protocol Label Switching) is a type of WAN technology that can be expensive. While it provides reliable and fast connections, it doesn't offer the cost-saving benefits or flexibility of SD-WAN.

Option D is incorrect. DMZ (Demilitarized Zone) is a buffer zone between an organization's internal network and the external, untrusted networks. It is not related to WAN connectivity or cost reduction.

Question 237. A financial company wants to improve its web browsing security by intercepting and inspecting web traffic to prevent users from accessing malicious sites or downloading malware. They are looking for a solution that can act as an intermediary for requests from clients seeking resources from other servers. What should the company implement?

- (A) Network IDS
- (B) VPN Concentrator
- (C) **Proxy server**
- (D) Jump server

Explanation 237. Correct Answer: C. Proxy server. A Proxy server serves as an intermediary between the user's computer and the internet. It intercepts web requests and can provide functions such as filtering web content, caching web requests, and inspecting traffic for security reasons.

Option A is incorrect. A Network Intrusion Detection System (IDS) monitors and detects malicious activities on a network but does not function as an intermediary for web requests.

Option B is incorrect. A VPN Concentrator provides secure remote access to an organization's network but doesn't act as an intermediary for web browsing requests.

Option D is incorrect. A Jump server is used for secure and auditable access to internal servers but isn't designed for intercepting web traffic.

Question 238. In an IaaS (Infrastructure as a Service) model, which of the following tasks is typically the responsibility of the cloud customer in a standard Cloud Responsibility Matrix?

- (A) Physical security of data centers
- (B) Patching of host operating systems
- (C) Network infrastructure maintenance
- (D) **Patching of guest operating systems**

Explanation 238. Correct Answer: D. Patching of guest operating systems. In an IaaS model, the customer is typically responsible for managing their own virtual machines, which includes patching the guest operating systems. The cloud provider is generally responsible for the physical infrastructure, network, and the host operating system.

Option A is incorrect. Physical security of data centers is the responsibility of the cloud provider. The customer does not have control over the physical infrastructure in a cloud environment.

Option B is incorrect. Patching of host operating systems is the cloud provider's responsibility. They manage the underlying infrastructure, including the host systems.

Option C is incorrect. Maintenance of network infrastructure is typically handled by the cloud provider, ensuring connectivity and uptime for the resources they offer.

Question 239. In a cloud environment, which of the following matrices defines the shared responsibilities between the cloud provider and the customer for specific cloud service models?

- (A) Shared Accountability Matrix
- (B) Cloud Resource Allocation Table
- (C) Cloud Security Posture Matrix
- (D) **Cloud Responsibility Matrix**

Explanation 239. Correct Answer: D. Cloud Responsibility Matrix. The Cloud Responsibility Matrix defines the shared responsibilities between the cloud provider and the customer in a cloud environment, delineating what security measures the provider will handle and which ones are the responsibility of the customer.

Option A is incorrect. While the term “Shared Accountability Matrix” may sound relevant, there’s no standard matrix in cloud computing with this name. Shared responsibility is the concept, but the actual term used in the context of cloud security is the “Cloud Responsibility Matrix.”

Option B is incorrect. A “Cloud Resource Allocation Table” is not a standard term associated with delineating responsibilities in the cloud. It sounds more related to how resources, such as compute or storage, might be allocated.

Option C is incorrect. “Cloud Security Posture Matrix” is not a recognized term for defining shared responsibilities in cloud environments. Instead, it sounds more like a potential term for an organization’s stance or positioning regarding cloud security.

Question 240. A financial organization collects and stores personally identifiable information (PII) of its customers. The company operates within jurisdictions that have strict regulations concerning the storage, transmission, and processing of such data. Which of the following strategies would be MOST appropriate for the company to ensure compliance with these regulations?

- (A) Use open source encryption algorithms without validation
- (B) Only store customer data in physical, on-site servers
- (C) **Implement data classification and labeling procedures**
- (D) Limit the number of administrators with access to the data

Explanation 240. Correct Answer: C. Implement data classification and labeling procedures. By implementing data classification and labeling procedures, the organization can clearly identify which data is regulated, ensuring appropriate controls, access rights, and protective measures are in place. This aids in achieving compliance by setting clear guidelines on data handling based on the classification.

Option A is incorrect. While encryption is essential for protecting sensitive data, using open source algorithms without validation might not ensure that the data is protected to the standards required by regulations.

Option B is incorrect. Storing customer data only on physical, on-site servers doesn't necessarily guarantee compliance.

Regulations often require specific controls regardless of where the data is stored.

Option D is incorrect. While limiting administrative access can reduce the risk of insider threats, it doesn't directly ensure that the regulated data is handled in compliance with legal requirements.

Question 241. During an annual review, a company discovered that one of its critical systems had several unscheduled downtimes over the year. The CTO has recommended a move towards high availability architecture to address this. What is the PRIMARY concern when implementing high availability?

- (A) Ensuring that there are no single points of failure
- (B) Ensuring that the system is patched regularly
- (C) Implementing multi-factor authentication
- (D) Storing backups in multiple geographical locations

Explanation 241. Correct Answer: A. Ensuring that there are no single points of failure. In a high availability (HA) system, eliminating single points of failure is of utmost importance. By ensuring redundancy at every potential failure point, the system can remain operational even if a component fails.

Option B is incorrect. While patching is important for security, it is not the primary concern when implementing high availability.

Option C is incorrect. Multi-factor authentication is essential for secure access but does not directly relate to high availability architecture.

Option D is incorrect. Having backups in various geographical locations is more relevant to disaster recovery than to high availability.

Question 242. After a recent service outage, a hospital's IT team is reviewing the availability of its patient record system. They want to ensure the system remains operational, even in the event of hardware failures. Which of the following considerations is MOST relevant to this requirement?

- (A) **Implementing database mirroring**
- (B) Regularly updating the system's antivirus definitions
- (C) Using strong encryption for data at rest
- (D) Conducting penetration testing on the system

Explanation 242. Correct Answer: A. Implementing database mirroring. Database mirroring is a solution for increasing the availability of a SQL Server database. Mirroring is implemented on a per-database basis and works only with databases that use the full recovery model. This ensures that in the event of a hardware failure, there's a mirrored copy of the data available.

Option B is incorrect. While updating antivirus definitions is crucial for preventing malware infections, it is not directly

related to ensuring high availability in the face of hardware failures.

Option C is incorrect. Encryption is vital for data security but doesn't directly address the high availability needs of a system.

Option D is incorrect. Penetration testing identifies vulnerabilities in the system but doesn't provide a solution for high availability in case of hardware failures.

Question 243. An enterprise wants to configure its firewall so that if a malfunction occurs, the firewall should automatically allow traffic to ensure business continuity. Which failure mode should be implemented?

- (A) Fail-safe
- (B) Fail-over
- (C) Fail-closed
- (D) **Fail-open**

Explanation 243. Correct Answer: D. Fail-open. In a fail-open mode, when the system or device fails, it defaults to an "open" state, allowing traffic to pass through. This mode prioritizes availability over strict security.

Option A is incorrect. "Fail-safe" is a term that typically refers to a system's ability to default to a safe condition in case of a failure. However, in the context of firewalls and access control systems, "fail-open" or "fail-closed" are the preferred terms.

Option B is incorrect. "Fail-over" refers to switching to a backup system or component in the event of a failure. It doesn't

describe the behavior of allowing or denying traffic during a failure.

Option C is incorrect. Fail-closed means that when a malfunction occurs, the system would block all traffic by default, which is the opposite of what the enterprise wants.

Question 244. An organization with a single physical network infrastructure wants to separate the traffic of its finance department from that of the HR department. They do not want to set up entirely new physical networks but want to ensure that data packets from one department do not mix with the other's. What should the organization implement?

- (A) Air-gapped network
- (B) DMZ (Demilitarized Zone)
- (C) **VLAN (Virtual Local Area Network)**
- (D) VPN (Virtual Private Network)

Explanation 244. Correct Answer: C. VLAN (Virtual Local Area Network). A VLAN allows a network administrator to create a logical network within a physical network. This logical segmentation can separate the traffic of different departments, ensuring that data packets from one VLAN do not mix with another, effectively isolating them.

Option A is incorrect. An air-gapped network is a physically isolated network and would require setting up a new physical network.

Option B is incorrect. A DMZ is a buffer zone between a private network and external networks. It doesn't help in segmenting traffic within the internal network.

Option D is incorrect. A VPN is used to create secure connections over an unsecured network. It does not logically segment traffic within a single physical network.

Question 245. A large organization is considering deploying a solution that will allow employees to securely access company resources remotely using their personal devices. The organization wants a solution that can provide strong authentication and ensure that the data remains confidential during transit. Which technology should be adopted?

- (A) Kerberos
- (B) Remote Desktop Services (RDS)
- (C) **Remote Access VPN**
- (D) SNMP

Explanation 245. Correct Answer: C. Remote Access VPN. Remote Access VPN provides a secure connection from a remote device to an organization's internal network. It uses encryption to ensure data confidentiality and can also be set up with strong authentication methods.

Option A is incorrect. Kerberos is an authentication protocol that uses tickets to allow nodes to prove their identity in a network. While it provides strong authentication, it doesn't inherently provide a solution for remote access with encrypted communication.

Option B is incorrect. Remote Desktop Services (RDS) allows users to access a remote desktop or application. While it can be secured, it doesn't always ensure encryption during transit, especially if not paired with another technology like VPN.

Option D is incorrect. SNMP (Simple Network Management Protocol) is used for managing and monitoring network devices. It isn't related to providing secure remote access for users.

Question 246. An e-commerce company wants to ensure that their customers' credit card data remains confidential while in transit over the internet. They are seeking a protocol that can help in securing their website's communication. Which protocol would best fit this requirement?

- (A) IPSec
- (B) SSH
- (C) TLS
- (D) ICMP

Explanation 246. Correct Answer: C. TLS. Transport Layer Security (TLS) is a cryptographic protocol that ensures data confidentiality and integrity over the internet. Websites use TLS to secure all communications between their servers and web browsers, making it suitable for e-commerce platforms to secure sensitive customer data.

Option A is incorrect. IPSec is a suite of protocols that secures IP communications by encrypting and authenticating all IP packets. It is more commonly used for VPNs rather than securing web communications.

Option B is incorrect. SSH (Secure Shell) is primarily used for secure remote access to systems, not for securing web-based communications.

Option D is incorrect. ICMP (Internet Control Message Protocol) is used by network devices to send error messages and operational information, not for securing data in transit.

Question 247. A rapidly growing e-commerce platform has been facing intermittent downtimes, especially during sale events. To ensure high availability and even distribution of traffic among servers, the company is considering deploying a specific type of network appliance. Which of the following should the company deploy?

- (A) Intrusion Detection System (IDS)
- (B) VPN concentrator
- (C) **Load balancer**
- (D) Proxy server

Explanation 247. Correct Answer: C. Load balancer. A load balancer is designed to distribute incoming network traffic across multiple servers to ensure that no single server is overwhelmed with too much traffic. This helps in ensuring high availability and optimizing resource utilization.

Option A is incorrect. An Intrusion Detection System (IDS) is primarily used for detecting malicious activities in the network, not for distributing traffic among servers.

Option B is incorrect. A VPN concentrator is used to create and manage VPN connections, not for balancing load among servers.

Option D is incorrect. While a proxy server can distribute client requests to different servers, its primary role is to act as an intermediary, not to ensure high availability or evenly distribute traffic.

Question 248. An organization is transitioning its IT infrastructure to be cloud-centric and aims to adopt a zero-trust network approach. They are looking for a solution that integrates cloud security, zero-trust access, and WAN capabilities, ensuring employees have consistent secure access regardless of their location. Which of the following best addresses their needs?

- (A) Remote Desktop Services (RDS)
- (B) **Secure access service edge (SASE)**
- (C) Content Delivery Network (CDN)
- (D) Virtual Local Area Network (VLAN)

Explanation 248. Correct Answer: B. Secure access service edge (SASE). SASE integrates multiple network and security functions traditionally delivered in separate point solutions. This includes capabilities such as Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall-as-a-Service (FWaaS), and Zero Trust Network Access (ZTNA), all delivered from a globally distributed set of cloud-native platforms.

Option A is incorrect. Remote Desktop Services (RDS) enables users to connect to a graphical interface of a remote

computer, but it doesn't inherently combine cloud security, zero-trust access, and WAN capabilities like SASE.

Option C is incorrect. A Content Delivery Network (CDN) is designed to deliver web content and web applications to users based on their geographical location. It doesn't provide integrated cloud security and WAN capabilities.

Option D is incorrect. A Virtual Local Area Network (VLAN) segments a physical network into multiple isolated networks. It doesn't offer the combined benefits of cloud security, zero-trust access, and WAN capabilities like SASE.

Question 249. A medium-sized e-commerce company recently experienced a data breach due to an external attack. Post-incident analysis revealed that while there were indications of the attack in their network traffic, no alarms were raised at the time of the attack. The company now wants to implement a solution to actively monitor and take action against malicious network traffic. Which of the following should they deploy?

- (A) Intrusion Detection System (IDS)
- (B) Network Access Control (NAC)
- (C) Proxy server
- (D) **Intrusion Prevention System (IPS)**

Explanation 249. Correct Answer: D. Intrusion Prevention System (IPS). An Intrusion Prevention System (IPS) not only detects malicious network activities but also takes active steps to prevent or block them, which is ideal for a company looking to bolster its defenses against real-time threats.

Option A is incorrect. An Intrusion Detection System (IDS) will detect and alert on malicious activity but does not take active steps to prevent the threat.

Option B is incorrect. Network Access Control (NAC) is primarily used for controlling network access based on policies, not for active monitoring and prevention of malicious network traffic.

Option C is incorrect. A Proxy server acts as an intermediary for requests from clients seeking resources but is not specifically designed to detect or prevent intrusions.

Question 250. GreenTech, a data center company, is planning to expand its operations in a region known for frequent power outages. To maintain security posture and ensure continuity of operations, which of the following should be their PRIMARY consideration regarding power?

- (A) Using power-efficient servers to reduce electricity costs
- (B) Setting up solar panels to promote green energy
- (C) **Investing in redundant power supplies and uninterruptible power systems (UPS)**
- (D) Running operations only during peak daylight hours to ensure natural lighting

Explanation 250. Correct Answer: C. Investing in redundant power supplies and uninterruptible power systems (UPS). Given the frequent power outages in the region, having redundant power supplies and UPS ensures that operations continue smoothly without abrupt interruptions,

which can lead to system crashes, data corruption, or security breaches.

Option A is incorrect. While power-efficient servers can reduce costs, they do not address the primary concern of power outages and maintaining operations.

Option B is incorrect. Solar panels promote green energy but might not provide consistent and immediate power backup during outages, especially during nighttime or cloudy days.

Option D is incorrect. Limiting operations to daylight hours is not a practical solution for a data center, as it restricts operational capacity and doesn't directly address the issue of power outages.

Question 251. A startup company anticipates rapid growth in its user base over the next year. They are considering an architectural model for their application that can handle the projected growth without performance issues. Which of the following would be the BEST design consideration for this situation?

- (A) Implementing strict password policies
- (B) Using a monolithic application design
- (C) Integrating a DDoS protection mechanism
- (D) **Adopting a microservices architecture**

Explanation 251. Correct Answer: D. Adopting a microservices architecture. Microservices architecture breaks down an application into small, independent services that run as

separate processes. This allows for better scalability as each service can be scaled individually based on the demand.

Option A is incorrect. While strict password policies are good for security, they don't directly address the scalability concerns of the application architecture.

Option B is incorrect. Monolithic designs are often harder to scale as changes or scaling in one area can affect the entire application.

Option C is incorrect. While DDoS protection is essential for defending against certain types of cyberattacks, it doesn't address the scalability of the application's core architecture.

Question 252. A healthcare provider is updating its network infrastructure. Due to the sensitive nature of the medical data they handle, they want to ensure that any anomalies or malicious activities in the network are immediately detected and alerted. Which system should they primarily consider?

- (A) Intrusion Prevention System (IPS)
- (B) **Intrusion Detection System (IDS)**
- (C) DHCP server
- (D) VPN concentrator

Explanation 252. Correct Answer: B. Intrusion Detection System (IDS). An Intrusion Detection System (IDS) actively monitors network traffic for any signs of malicious activities or policy violations and alerts the administrators. It is suitable for organizations that want to ensure anomalies are promptly detected.

Option A is incorrect. An Intrusion Prevention System (IPS) does actively monitor and detect malicious traffic but also takes measures to prevent it. While an IPS could be beneficial for the healthcare provider, the primary requirement mentioned was for detection and alerting, which is the primary function of an IDS.

Option C is incorrect. A DHCP (Dynamic Host Configuration Protocol) server assigns IP addresses to devices in a network. It does not monitor or alert on malicious network activities.

Option D is incorrect. A VPN concentrator is used to create and manage VPN connections, providing secure access to a network, but it doesn't primarily detect intrusions.

Question 253. The IT security team at a large corporation is evaluating monitoring tools for network traffic. They need a solution that can inspect network packets without introducing any potential latency or altering the network flow. Which type of device attribute should they consider?

- (A) Active IDS
- (B) Passive firewall
- (C) Active firewall
- (D) **Passive IDS**

Explanation 253. Correct Answer: D. Passive IDS. Passive IDS (Intrusion Detection System) is designed to monitor and analyze network traffic without influencing the traffic flow or causing potential latency. It observes traffic in real-time but doesn't take active actions on its own.

Option A is incorrect. An Active IDS can detect potential security breaches and take action, which may introduce latency or alter the traffic flow.

Option B is incorrect. While the term “passive firewall” is not standard, traditional firewalls can actively block or allow traffic, which can introduce changes to the network flow.

Option C is incorrect. An Active firewall actively filters network traffic based on configured policies, potentially affecting the network flow.

Question 254. A developer at your company is excited about the scalability benefits of serverless architecture and has deployed a new service using it. However, you notice an increased bill due to the service even when it’s not in use. Which of the following could be a contributing factor?

- (A) The serverless functions are continuously triggered by unintended events**
- (B)** The server hardware is outdated
- (C)** The load balancer is misconfigured
- (D)** The organization lacks a Content Delivery Network (CDN)

Explanation 254. Correct Answer: A. The serverless functions are continuously triggered by unintended events. Serverless architectures charge based on the number of function invocations and the execution time. If there are unintended events, such as rogue requests or misconfigured triggers, continuously invoking the serverless functions, it could lead to unexpected costs.

Option B is incorrect. In a serverless architecture, the responsibility of server hardware management lies with the service provider. The customer is abstracted from the hardware details.

Option C is incorrect. A misconfigured load balancer might affect availability or performance but is not directly related to unexpected cost hikes in a serverless deployment.

Option D is incorrect. While CDNs are valuable for optimizing content delivery, they are not directly related to the cost implications of unintended function invocations in a serverless architecture.

Question 255. After a recent security breach, CyberCorp is reviewing its software vendors for their responsiveness to vulnerabilities. Which of the following metrics would BEST assist CyberCorp in determining the timeliness and efficiency of security patches from a vendor?

- (A) The frequency of software updates released by the vendor
- (B) The vendor's quarterly financial reports
- (C) **Time between vulnerability disclosure and patch release by the vendor**
- (D) The number of features added by the vendor in the last software update

Explanation 255. Correct Answer: C. Time between vulnerability disclosure and patch release by the vendor. The time taken by a vendor to release a security patch after a vulnerability is disclosed is a direct measure of their

responsiveness to security threats. A shorter duration indicates a higher prioritization of security concerns.

Option A is incorrect. Frequency of software updates does not necessarily correlate with timely security patches. A vendor might release frequent updates but still be slow in addressing security issues.

Option B is incorrect. A vendor's quarterly financial reports might indicate the financial health of the company but does not directly reflect their responsiveness to security vulnerabilities.

Option D is incorrect. The number of features added in a software update does not indicate the timeliness or effectiveness of security patches.

Question 256. XYZ Corp. has recently developed a new manufacturing process that reduces production costs by 50%. This process is not yet patented and is considered a trade secret. The company wants to ensure that employees do not disclose this process to competitors. Which of the following would be the MOST effective strategy to achieve this?

- (A) Providing employees with a bonus for keeping the process confidential
- (B) Conducting random checks of employee communications
- (C) **Implementing a mandatory non-disclosure agreement (NDA) for all employees**
- (D) Hosting quarterly seminars to educate employees about the value of the trade secret

Explanation 256. Correct Answer: C. Implementing a mandatory non-disclosure agreement (NDA) for all employees. An NDA is a legally binding contract that prohibits employees from disclosing confidential information, like trade secrets. If an employee breaches the NDA, the company has legal grounds to seek damages or other remedies.

Option A is incorrect. While bonuses might provide an incentive for employees, it doesn't provide a binding legal framework to protect the trade secret.

Option B is incorrect. Random checks can deter some employees but might not be effective across the board and could also lead to trust issues within the organization.

Option D is incorrect. While education is essential and can instill a sense of responsibility, it doesn't provide a legal means to protect the trade secret as an NDA does.

Question 257. A large e-commerce platform is facing challenges during peak sale periods, where the influx of users causes slowdowns and occasional outages. Which of the following solutions would BEST improve scalability during these high-demand times?

- (A) Implement a centralized logging system
- (B) **Employ auto-scaling cloud solutions**
- (C) Increase the frequency of data backups
- (D) Mandate regular security training for employees

Explanation 257. Correct Answer: B. Employ auto-scaling cloud solutions.

Auto-scaling in cloud solutions automatically adjusts the number of computational resources based on the actual demand. During peak periods, resources can be automatically increased to handle the demand, ensuring the system remains scalable and responsive.

Option A is incorrect. A centralized logging system is beneficial for monitoring and troubleshooting, but it does not directly address scalability during peak times.

Option C is incorrect. Increasing the frequency of data backups is a good practice for data integrity and recovery but does not handle scalability concerns directly.

Option D is incorrect. Regular security training is crucial for a company's cybersecurity posture, but it does not address the architectural scalability of the platform.

Question 258. An e-commerce company is preparing for an upcoming Black Friday sale, expecting a surge in web traffic. To ensure their systems remain responsive during the sale, which of the following would be the MOST effective strategy to implement?

- (A) Increasing password complexity for all users
- (B) Limiting the number of products on sale
- (C) **Implementing a content delivery network (CDN)**
- (D) Conducting a yearly security audit

Explanation 258. Correct Answer: C. Implementing a content delivery network (CDN). CDNs distribute the traffic load among multiple servers, often geographically dispersed.

This not only speeds up content delivery to users but also helps in handling traffic surges, ensuring the system remains responsive during high-demand periods such as Black Friday sales.

Option A is incorrect. Increasing password complexity can enhance security but does not directly impact system responsiveness during high traffic periods.

Option B is incorrect. Limiting the number of products on sale may reduce server load, but it might also decrease potential revenue and is not a direct method for improving system responsiveness.

Option D is incorrect. While yearly security audits are essential for identifying vulnerabilities, they don't directly address system responsiveness during high traffic periods.

Question 259. A multinational corporation has data centers located in different countries. Due to regulatory constraints, remote access to these data centers is highly restricted. The company's IT administrators need a centralized way to access all data centers securely without directly accessing them from their workstations. Which solution should the company consider?

- (A) Setting up a DMZ
- (B) **Implementing a Jump server**
- (C) Deploying an Active Directory
- (D) Using a local Proxy

Explanation 259. Correct Answer: B. Implementing a Jump server. A Jump server, also known as a bastion host, acts as an intermediary server allowing users to connect to it before accessing another server or network. It provides a controlled means of access between two networks, such as an internal network and an external network.

Option A is incorrect. A DMZ (Demilitarized Zone) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually the internet. It doesn't provide a consolidated access point like a Jump server.

Option C is incorrect. Active Directory is a directory service for Windows domain networks. It's not designed to provide controlled remote access to multiple data centers.

Option D is incorrect. A local Proxy might be used to control internet access or cache web content but doesn't act as a centralized access point for data centers like a Jump server.

Question 260. Acme Corp is restructuring its internal network to improve its security posture. They aim to separate areas with different levels of trust. Which of the following approaches would BEST achieve this objective?

- (A) Implementing VLANs based on organizational departments
- (B) Setting up a perimeter firewall to segment external and internal traffic
- (C) **Designing network zones based on data sensitivity**

and access requirements

(D) Using a single, flat network for simplicity

Explanation 260. Correct Answer: C. Designing network zones based on data sensitivity and access requirements.

Zoning based on data sensitivity and access requirements ensures that segments of the network with varying trust levels are isolated. This reduces the risk of a breach in one zone affecting another.

Option A is incorrect. While VLANs can segment traffic, doing so based purely on organizational departments may not align with varying trust and data sensitivity requirements.

Option B is incorrect. While perimeter firewalls are crucial for security, they primarily separate internal from external traffic and don't segment areas of varying trust within the internal network.

Option D is incorrect. A single, flat network doesn't provide segmentation, making it vulnerable to lateral movement if a threat actor gains access.

Question 261. Your organization is implementing Infrastructure as Code (IaC) to deploy and manage its cloud infrastructure. As part of a security review, what is a primary concern regarding the use of IaC scripts?

(A) Lack of graphical interface for infrastructure visualization

(B) Hardcoding sensitive data within the scripts

- (C) Inability to scale the infrastructure dynamically
- (D) Incompatibility with non-cloud environments

Explanation 261. Correct Answer: B. Hardcoding sensitive data within the scripts. Infrastructure as Code (IaC) scripts are meant to automate infrastructure deployment. If sensitive data such as passwords or API keys are hardcoded into these scripts, they could be exposed, leading to potential security breaches. It's essential to use secure methods, like secrets management or encrypted variables, to handle sensitive data.

Option A is incorrect. While IaC focuses on code-driven infrastructure management, many tools provide ways to visualize the infrastructure or are compatible with tools that do.

Option C is incorrect. One of the benefits of IaC is the ability to scale infrastructure dynamically. It allows for automated scaling based on the script or configuration files.

Option D is incorrect. IaC can be used in various environments, not just cloud. It depends on the tool and the platform it supports.

Question 262. A cloud-based SaaS company wants to ensure its infrastructure can handle a potential influx of a large number of users in the future. Which of the following approaches would BEST meet this scalability consideration?

- (A) **Implement a horizontal scaling strategy**
- (B) Introduce multi-factor authentication
- (C) Deploy deep packet inspection tools
- (D) Implement a centralized logging system

Explanation 262. Correct Answer: A. Implement a horizontal scaling strategy. Horizontal scaling involves adding more machines or nodes to a system to handle increased load, which can be especially effective in a cloud environment. It allows the infrastructure to accommodate more users by distributing the load among multiple servers.

Option B is incorrect. Multi-factor authentication is essential for security, but it does not address the scalability of the infrastructure to handle a large number of users.

Option C is incorrect. Deep packet inspection tools are used for analyzing network traffic for security and management purposes, but they don't directly enhance the scalability of an infrastructure.

Option D is incorrect. Centralized logging systems help consolidate and analyze logs from various sources, but they do not address the scalability needs of the infrastructure itself.

Question 263. A software development company is looking to migrate its legacy applications to a more modern infrastructure. They want to ensure the applications can be deployed consistently across multiple environments without the challenges of varying dependencies and configurations. Which approach would best achieve this goal?

- (A) Virtual Machine Deployment
- (B) Bare-Metal Deployment
- (C) **Containerization**
- (D) Serverless Computing

Explanation 263. Correct Answer: C. Containerization

Containerization encapsulates an application and its dependencies into a ‘container.’ This allows the application to be consistently deployed across different environments regardless of variations in configurations or dependencies.

Option A is incorrect. While virtual machines provide an isolated environment for applications, they include the overhead of an entire guest OS and don’t directly address the challenge of application dependencies varying across environments.

Option B is incorrect. Bare-metal deployment involves installing applications directly on hardware without virtualization or containers. This method does not inherently ensure consistent deployment across multiple environments.

Option D is incorrect. Serverless computing abstracts the infrastructure away from the developer, focusing on individual functions. While it provides scalability and simplicity, it doesn’t directly address consistent deployment across environments due to dependencies and configurations.

Question 264. A large enterprise is considering a transition to a more flexible and programmable network architecture. They want to centralize the control plane, allowing for automated, programmable network configurations and rapid provisioning. Which network architecture model should they consider?

- (A) VLAN (Virtual Local Area Network)
- (B) MPLS (Multiprotocol Label Switching)
- (C) VPN (Virtual Private Network)
- (D) **SDN (Software-Defined Networking)**

Explanation 264. Correct Answer: D. SDN (Software-Defined Networking). Software-Defined Networking (SDN) centralizes the control plane, decoupling it from the data plane. This allows for a more flexible and programmable network, enabling automated configurations, and rapid provisioning.

Option A is incorrect. A VLAN is used to create logical networks within a physical network but doesn't provide centralized control or programmability across the entire network.

Option B is incorrect. MPLS is a type of data-carrying technique for high-performance telecommunications networks. It doesn't centralize network control or enhance programmability as SDN does.

Option C is incorrect. A VPN is designed to provide a secure tunnel between networks over potentially insecure mediums like the internet. It does not offer the centralized, programmable configuration benefits of SDN.

Question 265. A global corporation has undergone several IT incidents in the past year, including outages due to natural disasters and cyber attacks. The CEO wants to ensure the organization's IT infrastructure can withstand or rapidly recover from disruptive events. Which of the following best encapsulates this requirement?

- (A) Adopting a Zero Trust Architecture
- (B) Implementing a strict password policy
- (C) Establishing a Business Continuity Plan (BCP) with

emphasis on resilience

(D) Regularly updating firewall rules

Explanation 265. Correct Answer: C. Establishing a Business Continuity Plan (BCP) with emphasis on resilience.

Resilience in this context refers to the ability of the IT infrastructure to rapidly recover and continue functioning even after disruptive events. A Business Continuity Plan with a focus on resilience would help the organization prepare for, respond to, and recover from both natural and man-made incidents.

Option A is incorrect. Zero Trust Architecture emphasizes not trusting any user or system, both inside and outside the perimeter, but it doesn't address resilience against disruptive events directly.

Option B is incorrect. While password policies are essential for security, they are not centered around ensuring resilience against disruptive events.

Option D is incorrect. Updating firewall rules is crucial for keeping out unwanted traffic and potential threats but doesn't directly address the resilience of an IT infrastructure against major disruptive events.

Question 266. A medical company has recently deployed a device to monitor patient heart rates in real time. This device uses a real-time operating system (RTOS) to guarantee immediate response times. The security team is concerned about potential risks. Which of the following would be a KEY

recommendation to enhance the security of such devices?

- (A) Ensure real-time data analysis capabilities
- (B) Integrate the device with the corporate cloud for backups
- (C) **Implement strict network segmentation for the device**
- (D) Increase the storage capacity of the device

Explanation 266. Correct Answer: C. Implement strict network segmentation for the device. To protect RTOS devices, which often prioritize performance over security, it's crucial to minimize their exposure to potential threats. By segmenting the network, you can isolate the device from other systems and reduce the risk of a security incident.

Option A is incorrect. Real-time data analysis is more about performance and functionality than security.

Option B is incorrect. Integrating the device with the corporate cloud could introduce more security concerns, especially if the cloud environment is not secured properly.

Option D is incorrect. Storage capacity is a matter of device functionality, not a direct security enhancement for an RTOS device.

Question 267. A small business wants to deploy a single network security device that can handle multiple security functions such as firewall protection, intrusion detection, anti-malware, and content filtering. Which of the following would be the most suitable solution?

- (A) Network Intrusion Detection System (NIDS)
- (B) Web Application Firewall (WAF)
- (C) **Unified Threat Management (UTM)**
- (D) Proxy Server

Explanation 267. Correct Answer: C. Unified Threat Management (UTM). Unified Threat Management (UTM) devices are designed to combine multiple security features into a single appliance. This makes them ideal for smaller organizations that require a comprehensive range of security functions but might not have the resources to deploy and manage multiple standalone devices.

Option A is incorrect. While NIDS can identify and notify of potential malicious activities, it does not offer the comprehensive multi-feature capabilities found in a UTM.

Option B is incorrect. A Web Application Firewall (WAF) specifically protects web applications from certain types of attacks like XSS and SQL injection. It does not encompass the broader range of security functions that a UTM does.

Option D is incorrect. A Proxy Server primarily controls internet access and might provide some caching and content filtering capabilities, but it doesn't offer the wide range of security functions that a UTM does.

Question 268. An e-commerce company is experiencing attacks that specifically target the shopping cart feature of its web application. They want to implement a firewall that can understand web application-specific commands and provide

protection. Which type of firewall should they consider?

- (A) Layer 4 Firewall
- (B) Layer 2 Firewall
- (C) **Layer 7 Firewall**
- (D) Packet Filtering Firewall

Explanation 268. Correct Answer: C. Layer 7 Firewall.

Layer 7 firewalls, often known as Application Layer firewalls, can understand and filter traffic based on application-specific data, commands, or functions. They operate at the highest layer in the OSI model and can make decisions based on the actual content of the traffic.

Option A is incorrect. Layer 4 firewalls, also known as transport layer firewalls, primarily deal with data based on port numbers and protocol. They wouldn't be as effective in filtering application-specific commands as a Layer 7 firewall.

Option B is incorrect. Layer 2 firewalls operate at the data link layer, primarily dealing with MAC addresses. They aren't equipped to analyze application-specific content.

Option D is incorrect. Packet Filtering Firewalls operate primarily at the network layer, making decisions based on source/destination IP addresses, port numbers, and protocol types, not application-specific content.

Question 269. A financial organization's high-security data center has an authentication system for its main entry. If the system encounters an unexpected error, the organization wants to ensure that no one can gain access to the data center until the

system is fixed. Which configuration should the authentication system be set to?

- (A) Fail-open
- (B) **Fail-closed**
- (C) Fail-secure
- (D) Fail-passive

Explanation 269. Correct Answer: B. Fail-closed. Fail-closed, also known as fail-secure, is a mode where if a system fails, it denies all requests by default, effectively “closing” access. In high-security environments, it’s often preferred to prevent any unauthorized access during system failures.

Option A is incorrect. Fail-open is the opposite of what the organization wants. In a fail-open scenario, if the system fails, it would allow all requests by default.

Option C is incorrect. While “fail-secure” is another term for “fail-closed”, the use of both terms in the options can confuse the test-taker. In this context, option B is the more appropriate choice.

Option D is incorrect. Fail-passive isn’t a standard term in the context of authentication failure modes. Fail-open and fail-closed (or fail-secure) are the primary recognized terms.

Question 270. A multinational company wants to allow its remote employees to securely access the corporate intranet over the Internet. The company’s primary concern is to ensure data confidentiality and integrity during transit. Which solution should the company implement?

- (A) VLAN
- (B) VPN
- (C) NAC
- (D) DMZ

Explanation 270. Correct Answer: B. VPN. A Virtual Private Network (VPN) allows remote users to establish a secure connection to an organization's internal network over the public internet. It encrypts the data in transit, ensuring both confidentiality and integrity.

Option A is incorrect. A VLAN (Virtual Local Area Network) is used to segment network traffic within a local network, but it does not provide encryption or a method for secure remote access.

Option C is incorrect. NAC (Network Access Control) is a security solution that enforces policy on devices attempting to access network resources, but it doesn't inherently provide encrypted communication over the internet.

Option D is incorrect. DMZ (Demilitarized Zone) is a network segment that acts as a buffer between an organization's internal network and untrusted external networks. It doesn't provide encrypted communication for remote users.

Question 271. After conducting a business impact analysis, a local library determined that they could afford several days of downtime without a significant impact on their operations. They want a disaster recovery solution that offers a balance between cost and recovery capabilities. Which site consideration is the

most suitable for the library's needs?

- (A) Mobile site with a full set of IT equipment
- (B) Hot site with daily data replication
- (C) **Cold site**
- (D) Warm site with weekly backups

Explanation 271. Correct Answer: C. Cold site. A cold site is an offsite facility that is pre-configured to accept equipment and data backups but doesn't have any of its own. Given the library's tolerance for several days of downtime, a cold site would be a cost-effective solution that aligns with their recovery capabilities.

Option A is incorrect. A mobile site with a full set of IT equipment would be more suitable for immediate recovery needs and might be overkill for a library that can tolerate several days of downtime.

Option B is incorrect. A hot site with daily data replication would be more suited for businesses with a low tolerance for downtime and would likely be more expensive than the library's budget allows.

Option D is incorrect. Even though a warm site with weekly backups might seem like a viable option, a cold site would still be more cost-effective for the library given their tolerance for downtime.

Question 272. An online payment gateway is evaluating methods to enhance the security of its payment processing system. They want a solution that replaces sensitive cardholder

data with a unique identifier that has no intrinsic value by itself. Which method should they implement?

- (A) Hashing the card data
- (B) Encrypting the card data
- (C) Masking the card data
- (D) **Tokenizing the card data**

Explanation 272. Correct Answer: D. Tokenizing the card data. Tokenization involves replacing sensitive data with a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value.

Option A is incorrect. Hashing would produce a fixed-size string, which cannot be reversed to its original value, but it doesn't create a "token" that can be swapped back for the original data.

Option B is incorrect. Encryption translates data into another form, or code, so that only people with access to a secret key or password can read it. It does not replace the data with a unique identifier with no intrinsic value.

Option C is incorrect. Masking involves hiding parts of data, such as showing only the last four digits of a credit card number. It doesn't replace the data with a unique identifier.

Question 273. A software company is developing a new cloud-based application where clients can store and manage their customer contact details. The stored data does not include financial or medical information but does contain phone numbers and email addresses. How should this information be

classified?

- (A) Public
- (B) Restricted
- (C) **Sensitive**
- (D) Classified

Explanation 273. Correct Answer: C. Sensitive. Phone numbers and email addresses are considered Personally Identifiable Information (PII) and should be classified as sensitive since unauthorized access could lead to privacy violations or misuse.

Option A is incorrect. Public classification is for data that is intended for general access and holds no confidential information.

Option B is incorrect. Restricted typically applies to data that is more confidential than sensitive data, such as financial or strategic data.

Option D is incorrect. Classified is a more general term and can encompass various levels of data classification, including Top Secret, Secret, or Confidential, typically used in government sectors.

Question 274. Cybertech Corp. is reviewing its backup protocols to enhance security. They decided that before transferring backups to an offsite location, the data should be rendered unreadable to unauthorized individuals. Which backup strategy will ensure this requirement is met?

- (A) Use deduplication before storing backups

- (B) Store backups in proprietary formats
- (C) **Encrypt backups before transfer**
- (D) Compress backups using standard tools

Explanation 274. Correct Answer: C. Encrypt backups before transfer. Encryption transforms data into a format that can only be read by someone who possesses the decryption key. By encrypting backups before transferring, Cybertech Corp. ensures that even if unauthorized individuals access the backup data, they won't be able to understand its contents.

Option A is incorrect. Deduplication reduces the storage space required for backups by eliminating redundant data but doesn't make data unreadable to unauthorized individuals.

Option B is incorrect. Using proprietary formats may obscure the data for some unauthorized users, but it does not provide the robust protection encryption does.

Option D is incorrect. Compressing backups using standard tools optimizes storage but does not ensure data confidentiality.

Question 275. After a major power outage, TechWave Corp. wants to ensure their primary data center's operations can be swiftly and seamlessly shifted to another facility. The company wants this process to be automated and immediate to prevent any service interruption. What type of test should TechWave Corp. conduct to validate this functionality?

- (A) Conduct a vulnerability assessment on both data centers
- (B) **Execute a failover test**

- (C) Engage in a tabletop exercise
- (D) Perform a routine backup test

Explanation 275. Correct Answer: B. Execute a failover test.

A failover test involves simulating a failure in the primary system to ensure that the backup system can seamlessly take over without any service interruption. It helps in verifying the resilience and recovery capabilities of an organization's infrastructure.

Option A is incorrect. A vulnerability assessment identifies potential weaknesses in systems but does not test the seamless transition between primary and backup systems.

Option C is incorrect. A tabletop exercise is a discussion-based session and does not involve the live testing of systems or processes.

Option D is incorrect. A routine backup test ensures that backups can be restored successfully but does not test the immediate switchover capability between systems.

Question 276. A pharmaceutical company is working on a new drug formula that promises to revolutionize the treatment of a particular disease. The R&D team has detailed documentation on the components, procedures, and results of the drug trials. How should this documentation be classified to ensure that only the right people within the company have access?

- (A) Unclassified
- (B) Public

- (C) **Confidential**
- (D) Sensitive

Explanation 276. Correct Answer: C. Confidential. This drug formula and its documentation represent valuable intellectual property for the pharmaceutical company. To protect against theft, corporate espionage, or accidental disclosure, it should be classified as confidential to ensure limited, controlled access.

Option A is incorrect. Unclassified data doesn't require any special protection or confidentiality and is inappropriate for valuable intellectual property.

Option B is incorrect. Public classification would make the information accessible to everyone, which is not suitable for proprietary drug formulas.

Option D is incorrect. While the drug formula is sensitive information, the "Confidential" classification offers stricter controls and is more suitable for such valuable intellectual property.

Question 277. A software development company maintains a shared code repository. The company wants to ensure that only developers can make changes to the code, but testers should be able to view the code without modifying it. Which approach should be implemented?

- (A) Assign all employees read-only permissions
- (B) Provide testers with administrative rights
- (C) **Implement role-based access controls (RBAC)**
- (D) Use data encryption on the repository

Explanation 277. Correct Answer: C. Implement role-based access controls (RBAC). RBAC assigns permissions based on roles within an organization. Developers can be given a role that allows them to modify code, while testers are given a role that only allows them to read the code.

Option A is incorrect. Assigning read-only permissions to all employees will prevent developers from making necessary changes to the code.

Option B is incorrect. Providing testers with administrative rights would give them more access than necessary, potentially allowing them to modify the code.

Option D is incorrect. While data encryption ensures the confidentiality of the data, it does not address the need for specific permission levels for different user roles.

Question 278. A software development company has just expanded its team and wants to ensure that in the event of a disaster, they can resume operations within a day. However, they have a limited budget for disaster recovery. Which of the following disaster recovery site types would be the most suitable for the company's needs?

- (A) Hot site with hourly data replication
- (B) Cold site with monthly data backups
- (C) **Warm site with daily backups**
- (D) Offsite tape backups

Explanation 278. Correct Answer: C. Warm site with daily backups. For the software development company's need to

resume operations within a day, a warm site with daily backups would be ideal. The warm site has equipment and some level of data ready, which would facilitate a faster recovery compared to a cold site or just offsite backups.

Option A is incorrect. A hot site with hourly data replication might provide the quickest recovery, but it's also the most expensive option which may not align with the company's budget constraints.

Option B is incorrect. A cold site with monthly data backups would be cost-effective but might not allow for operations to resume within a day due to the time needed to set up equipment and restore the latest data.

Option D is incorrect. Offsite tape backups alone would not provide the infrastructure or equipment needed for quick recovery. It would also take considerable time to restore operations just from tape backups.

Question 279. A financial institution wants to ensure that if a cyber attacker gains unauthorized access to one section of their network, the attacker cannot easily move laterally to more sensitive parts of the network. Which method can help achieve this objective?

- (A) Deploying a honeypot in every segment
- (B) **Implementing network segmentation**
- (C) Applying encryption on all data traffic
- (D) Enabling two-factor authentication for all users

Explanation 279. Correct Answer: B. Implementing network segmentation. Network segmentation divides a network into multiple segments or subnets. Each segment operates independently and can have its own security and access controls. This means that if an attacker compromises one segment, they won't necessarily have access to other segments.

Option A is incorrect. A honeypot is a decoy system to attract potential attackers, but it doesn't prevent lateral movement within the network once an attacker has access.

Option C is incorrect. While encrypting data traffic ensures confidentiality, it doesn't prevent lateral movement within the network.

Option D is incorrect. Two-factor authentication strengthens access controls but doesn't inherently stop lateral movement within a network if an attacker gains access.

Question 280. DataFin, a financial analytics firm, experienced a minor fire incident in one of its server rooms. Fortunately, they had backups stored in another wing of the building, allowing for quick data recovery. However, management realizes that in a major disaster, both primary and backup data might be destroyed. To address this, which backup strategy should DataFin consider?

- (A) Mirror Backup
- (B) Local Storage Backup
- (C) Incremental Backup
- (D) **Offsite Backup**

Explanation 280. Correct Answer: D. Offsite Backup. Offsite Backup involves storing backup data in a different geographical location from the primary data. This ensures that even if a disaster impacts the primary location, the backup remains safe and can be used for recovery.

Option A is incorrect. Mirror Backup refers to a backup that is an exact copy of the source data. It doesn't specify the geographic location of the backup.

Option B is incorrect. Local Storage Backup typically means backups are stored within the same physical premises or close vicinity of the primary data, which wouldn't address DataFin's concern of potential data loss in a major disaster.

Option C is incorrect. Incremental Backup involves backing up only the data that has changed since the last backup, regardless of where it's stored. It doesn't address the concern of geographic separation.

Question 281. A healthcare organization with patients worldwide is planning to set up a backup site for its medical data repository. They have been advised to consider geographic dispersion as part of their disaster recovery plan. Which of the following reasons is the LEAST valid for geographic dispersion in this scenario?

- (A) Mitigate risks of regional natural disasters
- (B) Offer redundancy in case of local power outages
- (C) Benefit from varying peak load times in different regions
- (D) **Ensure faster access speeds for global patients**

Explanation 281. Correct Answer: D. Ensure faster access speeds for global patients. Geographic dispersion's primary goal in a disaster recovery context is resilience and redundancy, not necessarily optimizing access speeds. While having servers in different locations can enhance speed for local users, in the context of a backup site for disaster recovery, the primary focus is on availability and redundancy, not speed.

Option A is incorrect. Geographic dispersion can help mitigate risks associated with regional natural disasters by ensuring that backup sites aren't impacted by the same disaster that affects the primary site.

Option B is incorrect. Regional power outages can be mitigated by having backup sites in different locations.

Option C is incorrect. Geographic dispersion can allow organizations to manage and distribute load more effectively by leveraging off-peak times in different regions.

Question 282. A multinational corporation is expanding its operations in various countries. The company has decided to restrict access to its internal network based on geolocation to ensure that only employees from specific countries can access certain data. Which of the following would be the MOST appropriate solution to implement this requirement?

- (A) Deploy a VPN with multi-factor authentication
- (B) Use MAC address filtering on all company devices
- (C) **Implement a geolocation-based access control system**
- (D) Set up region-specific SSIDs for the company's Wi-Fi network

Explanation 282. Correct Answer: C. Implement a geolocation-based access control system. Geolocation-based access control systems determine users' physical locations and can grant or deny access based on predefined geographic boundaries. This solution is most fitting for restricting access based on country-specific requirements.

Option A is incorrect. While a VPN with multi-factor authentication improves security, it doesn't inherently restrict access based on geolocation.

Option B is incorrect. MAC address filtering restricts access based on device hardware addresses and not on geolocation.

Option D is incorrect. Region-specific SSIDs might limit Wi-Fi access in certain areas, but they don't enforce geolocation-based restrictions on a broader scale.

Question 283. DigitalFront, an e-commerce company, is expecting a surge in traffic during their upcoming annual sale event. They want to ensure that their website and applications can handle the anticipated increase in user activity without any performance degradation. Which of the following steps is MOST relevant to achieving this goal?

- (A) Increasing the frequency of security audits
- (B) **Implementing capacity planning specifically focused on technology**
- (C) Adopting multi-factor authentication for all users
- (D) Investing in advanced threat intelligence solutions

Explanation 283. Correct Answer: B. Implementing capacity planning specifically focused on technology.

Capacity planning with a focus on technology ensures that all technological resources, such as servers, bandwidth, storage, and software, are adequately prepared to handle the expected increase in load or traffic, ensuring smooth performance during peak periods.

Option A is incorrect. Security audits are important for identifying vulnerabilities, but they don't address the direct need for scaling technology resources to manage increased traffic.

Option C is incorrect. Multi-factor authentication improves security for users but does not aid in handling a surge in website traffic or user activity.

Option D is incorrect. Advanced threat intelligence solutions provide insights into potential threats, but they don't address technology scaling to accommodate increased traffic.

Question 284. DeltaTech, a financial institution, operates its primary site on a UNIX-based platform. For disaster recovery purposes, they are considering setting up a backup site on a different platform. Which of the following is NOT a primary benefit of introducing platform diversity in this case?

- (A) It reduces the organization's learning curve by using familiar technologies**
- (B) It provides resilience against attacks targeting UNIX-based systems**
- (C) It ensures that platform-specific outages don't affect**

both primary and backup sites

(D) It diversifies the attack surface, reducing the impact of specific platform vulnerabilities

Explanation 284. Correct Answer: A. It reduces the organization's learning curve by using familiar technologies.

Introducing a new platform usually increases the learning curve as staff need to be trained on the new system. The primary benefits of platform diversity are resilience, redundancy, and diversifying the attack surface.

Option B is incorrect. This is one of the benefits of platform diversity. If a vulnerability or threat targets UNIX-based systems, having a backup on a different platform ensures that the backup isn't compromised by the same threat.

Option C is incorrect. This is a benefit of platform diversity. Platform-specific outages or issues would only affect systems on that platform, so having a backup on a different platform adds resilience.

Option D is incorrect. This is one of the benefits of platform diversity. By using different platforms, the organization reduces the risk associated with vulnerabilities specific to a single platform.

Question 285. After a recent system upgrade, CloudTech Corp. decided to validate the efficiency and reliability of its new data processing system. To do this, they run the new system alongside the old one and compare the outcomes. This way, they aim to ensure that the new system is both robust and capable of

handling the current workload. What kind of testing is CloudTech Corp. utilizing?

- (A) Load Testing
- (B) Failover Testing
- (C) **Parallel Processing Testing**
- (D) Simulation Testing

Explanation 285. Correct Answer: C. Parallel Processing Testing. Parallel Processing Testing involves running two systems simultaneously (typically the new one and the old one) to compare the outcomes. This kind of testing ensures that a new system is as effective and reliable as the previous one.

Option A is incorrect. Load Testing checks the system's ability to handle the expected volume of transactions and to see if it can maintain acceptable response times.

Option B is incorrect. Failover Testing is done to ensure that a system can switch to a backup or secondary system in the case of a failure, rather than comparing two systems for consistency.

Option D is incorrect. Simulation Testing involves creating a model of the system under test and stimulating it with virtual users or devices to understand its behavior under various conditions.

Question 286. TechSolutions Inc., a rapidly growing startup, is expanding its workforce to meet its customer demands. As part of this expansion, they need to ensure their IT infrastructure can accommodate the influx of new employees without compromising performance or security. Which of the following

should be TechSolutions' primary focus during this expansion phase?

- (A) Adopting a Zero Trust Network Architecture
- (B) Increasing the frequency of vulnerability assessments
- (C) **Implementing capacity planning**
- (D) Deploying additional firewalls and intrusion detection systems

Explanation 286. Correct Answer: C. Implementing capacity planning. Capacity planning ensures that an organization's infrastructure, technology, and people are scaled appropriately to meet growth and performance needs. In the scenario, with an influx of new employees, ensuring that the IT infrastructure can handle the increased demand is crucial.

Option A is incorrect. While adopting a Zero Trust Network Architecture might enhance security, it doesn't address the need to scale resources to accommodate new employees.

Option B is incorrect. Vulnerability assessments are crucial for security, but they don't directly address the infrastructure's ability to handle growth.

Option D is incorrect. While firewalls and IDS can improve security, they don't directly address the organization's capacity to handle more employees

Question 287. StreamNet, a popular online streaming service, is planning to launch in three new countries. They anticipate a substantial increase in users and concurrent streams. To ensure that the service remains uninterrupted and provides a seamless

experience to new users, which action related to capacity planning should StreamNet prioritize?

- (A) Investing in content encryption and DRM
- (B) Increasing marketing and promotional activities in the new countries
- (C) Implementing stronger user authentication methods
- (D) **Expanding and optimizing their infrastructure to handle the projected growth**

Explanation 287. Correct Answer: D. Expanding and optimizing their infrastructure to handle the projected growth. Infrastructure capacity planning will allow StreamNet to predict the necessary resources required and make the needed upgrades or adjustments to their servers, networks, storage, and other infrastructure components. This ensures a smooth user experience even with the influx of new users.

Option A is incorrect. While content encryption and DRM (Digital Rights Management) are essential for protecting content, they don't address the infrastructure capacity needed to handle more users.

Option B is incorrect. Marketing and promotional activities can attract users but don't directly impact the infrastructure's capacity to support those users.

Option C is incorrect. Stronger authentication methods can improve security but don't address the capacity or scalability of the infrastructure.

Question 288. GlobalTech is implementing a disaster recovery plan and wants to ensure continuous availability with no data loss. They have decided to use replication as a backup strategy. Which of the following replication techniques should GlobalTech implement to achieve their objective?

- (A) Periodic replication scheduled daily
- (B) Asynchronous replication with hourly synchronization
- (C) **Synchronous replication**
- (D) Snapshot replication every 30 minutes

Explanation 288. Correct Answer: C. Synchronous replication. Synchronous replication ensures that data is written to the primary and secondary locations simultaneously, ensuring no data loss and continuous availability. This method is suitable for GlobalTech's requirement of no data loss.

Option A is incorrect. Periodic replication scheduled daily could result in up to a day's worth of data loss in the event of a disaster.

Option B is incorrect. Asynchronous replication with hourly synchronization could lead to an hour's worth of data loss if an incident occurs just before synchronization.

Option D is incorrect. Snapshot replication every 30 minutes could result in 30 minutes of data loss in the event of an incident.

Question 289. A software company has developed a new product. They want to release a user manual that details how to use the software, its features, and basic troubleshooting steps.

What should be the classification of this user manual?

- (A) Confidential
- (B) Restricted
- (C) **Public**
- (D) Internal

Explanation 289. Correct Answer: C. Public. A user manual is intended for all users of the software and should be easily accessible. It doesn't contain sensitive or proprietary information about the software's underlying code or algorithms. Hence, it should be classified as "Public."

Option A is incorrect. "Confidential" classification is too restrictive for a document meant to be distributed with every software copy and to guide users.

Option B is incorrect. "Restricted" would limit the distribution of the manual unnecessarily, making it harder for users to access the information they need.

Option D is incorrect. "Internal" classification would suggest the manual is only for internal company use, whereas it's intended for all users of the software.

Question 290. A global finance firm has recently faced downtime due to unexpected disasters in its main operational region. The firm wishes to have a backup site that would allow them to continue their operations with minimal downtime and no data loss. Which type of backup site would be the most appropriate for the firm?

- (A) Cold site

- (B) Warm site
- (C) **Hot site**
- (D) Mobile site

Explanation 290. Correct Answer: C. Hot site. A hot site is a fully operational offsite data center configured and ready to continue operations immediately after a disaster. It has all the necessary equipment and up-to-date data backups, making it ideal for scenarios where minimal downtime and no data loss are essential.

Option A is incorrect. A cold site is a backup facility with space and infrastructure but without updated equipment or data. It requires time to set up and is not suitable for immediate recovery.

Option B is incorrect. A warm site is a middle ground between a cold and hot site. It has some equipment and backups but will require more time to get fully operational compared to a hot site.

Option D is incorrect. A mobile site is usually a portable setup, often on a truck, that can be deployed to various locations. It might not be equipped for large-scale operations like a global finance firm would require.

Question 291. An international bank is setting up a new online portal for its customers to access their financial statements. Which measure should the bank implement to ensure that financial data in transit between the customer's browser and the bank's servers is kept confidential?

- (A) Use file-level encryption for all financial statements
- (B) Implement a Web Application Firewall (WAF)
- (C) **Use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for the portal**
- (D) Store all financial data in an encrypted database

Explanation 291. Correct Answer: C. Use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for the portal. SSL/TLS is designed to secure data in transit. By encrypting the data between the customer's browser and the bank's servers, it ensures the data's confidentiality while in transit.

Option A is incorrect. File-level encryption is great for data at rest but doesn't secure data in transit between a client and server.

Option B is incorrect. While a WAF can provide protection against web application attacks, it does not inherently encrypt data in transit.

Option D is incorrect. Storing financial data in an encrypted database safeguards the data at rest but doesn't ensure the confidentiality of data in transit to the client.

Question 292. A global e-commerce website wants to allow its customer service representatives to assist clients with order issues without exposing the full credit card details of the clients. Which method should the IT department employ to achieve this?

- (A) Replace all digits of the credit card number with random

characters

- (B) Display only the last four digits of the credit card number while masking the rest**
- (C)** Encrypt the credit card number with a symmetric key
- (D)** Use a hash function to represent the credit card number

Explanation 292. Correct Answer: B. Display only the last four digits of the credit card number while masking the rest.

Displaying only the last four digits and masking the rest ensures that customer service representatives have enough information to assist customers without being exposed to the entire credit card number.

Option A is incorrect. Replacing all digits with random characters would render the information useless for customer service representatives as they would not have any reference point.

Option C is incorrect. Encrypting the card number can protect the data, but the customer service representatives would need a way to decrypt it to access even partial information, defeating the purpose of not exposing them to the full details.

Option D is incorrect. Hashing the number would not allow any portion of the original data, like the last four digits, to be viewed, making it ineffective for this use case.

Question 293. XYZ Corp recently faced a ransomware attack that encrypted critical data files. The company's IT team was unable to decrypt the files but had a recent backup available. However, when they tried to restore the data, they found out the

backup was corrupted. Which of the following best practices would have helped XYZ Corp in ensuring the integrity of their backups?

- (A) **Regularly testing backup restoration processes**
- (B) Storing backups in the same directory as original files
- (C) Increasing the frequency of backups to every hour
- (D) Encrypting backups with a strong encryption algorithm

Explanation 293. Correct Answer: A. Regularly testing backup restoration processes. By regularly testing the restoration process from backups, organizations can identify and correct any issues with the backup files or processes before they are needed in a critical recovery situation.

Option B is incorrect. Storing backups in the same directory as the original files increases the risk of both the original and backup files being compromised or corrupted simultaneously.

Option C is incorrect. While increasing the frequency of backups can reduce data loss, it doesn't address the integrity or validity of the backups themselves.

Option D is incorrect. While encrypting backups provides security against unauthorized access, it doesn't ensure the integrity or usability of the backup.

Question 294. A financial institution is updating its infrastructure to ensure that customer financial data is kept secure from both internal and external threats. Which of the following would be the MOST effective measure to protect customer financial data from being accessed by unauthorized

internal users?

- (A) Deploying perimeter firewalls around the institution's network
- (B) Implementing two-factor authentication (2FA) for all customer accounts
- (C) **Enforcing strict access controls based on the principle of least privilege**
- (D) Conducting yearly cybersecurity awareness training for all employees

Explanation 294. Correct Answer: C. Enforcing strict access controls based on the principle of least privilege. The principle of least privilege (PoLP) ensures that users are given only the permissions they need to perform their job functions, nothing more. By enforcing strict access controls using this principle, the financial institution can minimize the risk of unauthorized internal users accessing sensitive financial data.

Option A is incorrect. Perimeter firewalls are more focused on preventing external threats and don't specifically address unauthorized internal access.

Option B is incorrect. Implementing 2FA is primarily for authenticating users and doesn't prevent unauthorized internal users from accessing data if they are already authenticated.

Option D is incorrect. While cybersecurity awareness training is crucial, it's not the most effective specific measure to prevent unauthorized internal access to financial data.

Question 295. A company's proprietary algorithm is being targeted by competitors aiming to replicate its functionality. To safeguard its intellectual property without changing the algorithm's behavior, the company wants a method that disguises the original code structure. What should they implement?

- (A) Data masking on the algorithm's output
- (B) **Obfuscation on the algorithm's code**
- (C) Encryption of the algorithm's storage location
- (D) Implementing a hashing mechanism within the algorithm

Explanation 295. Correct Answer: B. Obfuscation on the algorithm's code. Obfuscating the algorithm's code will make it more challenging to understand, reverse engineer, or replicate, without altering its behavior or results.

Option A is incorrect. Data masking on the algorithm's output would only hide or change certain parts of the output. It doesn't protect or disguise the algorithm's actual code or logic.

Option C is incorrect. Encrypting the algorithm's storage location protects the stored data from unauthorized access, but once accessed (e.g., for legitimate use), the original code structure would still be visible.

Option D is incorrect. Implementing a hashing mechanism within the algorithm might change its behavior and doesn't obscure the algorithm's logic or structure.

Question 296. A multinational e-commerce company is expanding its infrastructure to handle increasing traffic. The primary goal is to distribute the incoming web traffic across multiple servers to ensure that no single server is overwhelmed. Which method should the company use?

- (A) Deploy a web application firewall
- (B) Implement server clustering
- (C) Use hardware-based firewalls
- (D) **Set up a load balancer**

Explanation 296. Correct Answer: D. Set up a load balancer.

Load balancers distribute incoming traffic across multiple servers to ensure that no single server is overwhelmed, which enhances the availability and fault tolerance of applications.

Option A is incorrect. While a web application firewall can protect against web-based threats, it doesn't distribute incoming traffic across servers.

Option B is incorrect. Server clustering primarily focuses on providing redundancy and failover capabilities rather than distributing incoming traffic.

Option C is incorrect. Hardware-based firewalls are primarily used to filter traffic and protect networks from external threats, not to distribute incoming web traffic.

Question 297. A law firm is transitioning to a digital storage system and wants to ensure that client records and case files are protected from unauthorized access. Which of the following would be the BEST strategy to ensure the confidentiality of

legal information stored digitally?

- (A) Conducting regular penetration testing on the digital storage system
- (B) **Encrypting the client records and case files**
- (C) Applying watermarks to digital documents
- (D) Limiting physical access to the server room

Explanation 297. Correct Answer: B. Encrypting the client records and case files. Encryption is the process of converting information into an unreadable format unless one has the appropriate decryption key. By encrypting legal documents, unauthorized individuals, even if they gain access to the storage system, won't be able to comprehend the content of the documents.

Option A is incorrect. While regular penetration testing is essential to identify vulnerabilities in a system, it does not directly protect the confidentiality of stored legal information.

Option C is incorrect. Watermarking documents can deter copying or unauthorized distribution, but it doesn't prevent unauthorized access or reading of the documents.

Option D is incorrect. Limiting physical access to the server room can prevent unauthorized physical access, but it does not safeguard against digital breaches or protect the content of the files.

Question 298. A healthcare provider stores vast amounts of patient data on its servers. While they have strong perimeter defenses, they want an additional layer of security to ensure

patient data remains confidential even in the event of unauthorized access. Which of the following would be the MOST effective solution for this requirement?

- (A) Use hash algorithms on all patient data
- (B) Implement data deduplication techniques
- (C) **Encrypt the stored patient data**
- (D) Use a web application firewall (WAF)

Explanation 298. Correct Answer: C. Encrypt the stored patient data. Encrypting patient data ensures that even if malicious actors gain access to the data, they won't be able to understand or utilize it without the proper decryption key.

Option A is incorrect. Hashing is primarily used for verifying data integrity or storing passwords securely. Hashing would not allow the healthcare provider to retrieve and use the patient data when needed.

Option B is incorrect. Data deduplication is about reducing storage requirements by removing duplicate data; it doesn't provide confidentiality.

Option D is incorrect. While a WAF provides protection against web-based threats, it doesn't ensure the confidentiality of stored data in the event of unauthorized access.

Question 299. After a major outage, CloudTech Services is reviewing their disaster recovery strategy. The company found out that after restoring from backup, several applications did not function properly due to configuration discrepancies. What would be the best approach to ensure a successful recovery in

the future?

- (A) Prioritize applications for backup based on their importance
- (B) Implement differential backups in addition to full backups
- (C) **Regularly conduct a full system recovery in a test environment**
- (D) Use a third-party backup solution instead of an in-house solution

Explanation 299. Correct Answer: C. Regularly conduct a full system recovery in a test environment. By conducting a full system recovery in a test environment, CloudTech can simulate a real-world recovery scenario. This helps in identifying any discrepancies, configuration issues, or application dependencies that might be missed during regular backups, ensuring a successful recovery when it's critically needed.

Option A is incorrect. Prioritizing applications for backup based on their importance doesn't address the configuration discrepancies or interdependencies between applications.

Option B is incorrect. Implementing differential backups, while beneficial in capturing changes, does not address the configuration discrepancies found during the recovery.

Option D is incorrect. Using a third-party solution instead of an in-house solution does not inherently guarantee a successful recovery or address the specific issue of configuration discrepancies.

Question 300. A financial institution is implementing a system where customers can verify the integrity of their monthly statements without having access to the original data. Which of the following techniques would be MOST appropriate for this task?

- (A) Encrypting the statements using AES
- (B) Compressing the statements to reduce file size
- (C) **Hashing the statements and providing the hash value to the customers**
- (D) Tokenizing sensitive data within the statements

Explanation 300. Correct Answer: C. Hashing the statements and providing the hash value to the customers.

Hashing can be used to ensure data integrity. Customers can hash the statement they receive and compare it with the provided hash value to verify that the data hasn't been altered.

Option A is incorrect. While AES is a strong encryption method, encrypting the statements won't allow customers to verify the integrity of their statements. It ensures confidentiality more than integrity.

Option B is incorrect. Compressing the statements merely reduces the file size for ease of storage or transmission; it doesn't help in verifying data integrity.

Option D is incorrect. Tokenization replaces sensitive data with non-sensitive placeholders. It doesn't offer a way to verify the integrity of the entire statement.

Question 301. An organization has decided to focus on securing its database servers where customer details and transaction records are stored. This data is not being actively accessed or processed. Which type of security measure would be MOST appropriate for this type of data?

- (A) VLDData Loss Prevention (DLP) for emailAN
- (B) Web Application Firewall (WAF)
- (C) **Full Disk Encryption (FDE)**
- (D) Intrusion Detection System (IDS) for network traffic

Explanation 301. Correct Answer: C. Full Disk Encryption (FDE). Data at rest refers to data that is not actively moving through the network, such as data stored on hard drives. Full Disk Encryption (FDE) is a security measure specifically designed to protect data at rest by encrypting the entire hard drive.

Option A is incorrect. DLP for email primarily focuses on preventing unauthorized data transfers via email and is more suited for data in transit rather than data at rest.

Option B is incorrect. WAF protects web applications from various online threats and is not specifically tailored to protect data at rest.

Option D is incorrect. An IDS for network traffic mainly focuses on monitoring and detecting malicious activity in network traffic, which pertains to data in transit and not data at rest.

Question 302. A multinational company is considering using a cloud storage provider based in a foreign country to store customer data. The company's home country has strict data protection laws that require customer data to remain within its borders. Which of the following considerations is MOST critical for the company when choosing the cloud storage provider?

- (A) The speed of data access from the foreign-based cloud storage
- (B) The encryption standards used by the foreign cloud provider
- (C) **Whether the foreign cloud provider offers data storage exclusively within the company's home country**
- (D) The reputation and customer reviews of the foreign cloud provider

Explanation 302. Correct Answer: C. Whether the foreign cloud provider offers data storage exclusively within the company's home country. Data sovereignty refers to the concept that digital data is subject to the laws of the country in which it is located. If a company's home country has regulations that require customer data to stay within its borders, it's essential to ensure that the cloud provider offers storage that complies with this requirement.

Option A is incorrect. While speed of data access is important, it doesn't address the data sovereignty concern.

Option B is incorrect. While encryption is essential for security, it doesn't guarantee compliance with data sovereignty laws.

Option D is incorrect. Reputation is important, but it doesn't directly address the specific requirement of data sovereignty.

Question 303. After an annual review, BestTech Co. realized that their IT team was unfamiliar with the protocols to follow during a data breach. To ensure the team understands the steps and decision points without launching a live drill, what should the company implement?

- (A) Upgrade their firewall systems
- (B) **Engage in a tabletop exercise**
- (C) Conduct a red team exercise
- (D) Implement multi-factor authentication for all users

Explanation 303. Correct Answer: B. Engage in a tabletop exercise. Tabletop exercises allow teams to discuss and review specific scenarios, such as a data breach, and ensure everyone understands their roles and the processes to follow. It's a cost-effective way to familiarize the team with response procedures.

Option A is incorrect. Upgrading firewall systems may enhance the company's security posture but doesn't familiarize the IT team with data breach response protocols.

Option C is incorrect. A red team exercise is a live simulated attack to evaluate the organization's security posture and does not focus on walking the team through the response steps in a controlled environment.

Option D is incorrect. Multi-factor authentication is a security measure to validate users' identities but does not address the team's unfamiliarity with data breach response protocols.

Question 304. SecureData Inc., a financial firm, recently experienced a system crash and needed to restore their database. While they had a full backup from the previous week, they realized that several days of transactions were missing. To prevent such data loss in the future, which backup strategy involving recording transactions can SecureData implement?

- (A) Implement differential backups
- (B) Use snapshot backups every hour
- (C) **Enable database journaling**
- (D) Configure RAID 5 for their storage

Explanation 304. Correct Answer: C. Enable database journaling. Journaling involves keeping a log or ‘journal’ of every transaction or change that happens. If there’s a crash, the system can be restored to the last backup and then use the journal to replay each transaction, thus preventing data loss.

Option A is incorrect. Differential backups capture changes since the last full backup, but they don’t record every transaction in real-time like journaling.

Option B is incorrect. While hourly snapshot backups would reduce the potential data loss window, they still don’t capture every transaction in real-time.

Option D is incorrect. RAID 5 offers redundancy and can protect against a disk failure, but it doesn’t capture and record every database transaction like journaling.

Question 305. SecureNet Inc. recently upgraded their security infrastructure. To validate how the new system would respond

in real-world scenarios without exposing it to actual risks, they decide to imitate certain cyber threats in a controlled environment. Which type of test is SecureNet Inc. planning to conduct?

- (A) Penetration Testing
- (B) **Simulation Testing**
- (C) Vulnerability Assessment
- (D) Failover Testing.

Explanation 305. Correct Answer: B. Simulation Testing.

Simulation testing involves creating a model of the system under test and then stimulating it with virtual users or devices to understand its behavior under various conditions. In the context of cybersecurity, this means imitating cyber threats in a controlled environment to assess how security infrastructure responds.

Option A is incorrect. Penetration Testing involves ethical hackers attempting to breach an organization's defenses, which involves actual risks, rather than just a simulation.

Option C is incorrect. A Vulnerability Assessment identifies, quantifies, and prioritizes vulnerabilities in a system but doesn't necessarily imitate threats in a controlled environment.

Option D is incorrect. Failover Testing ensures that a system can switch to a backup or secondary system in case of a failure, and does not focus on simulating threats.

Question 306. ZenTech, a multinational corporation, recently adopted a multi-cloud strategy, deploying workloads across

multiple cloud service providers. What is a primary security benefit of this approach?

- (A) Centralized management of all cloud resources
- (B) Automatic encryption of data in transit between clouds
- (C) **Mitigation against a single point of failure**
- (D) Reduction in the cost of cloud storage solutions

Explanation 306. Correct Answer: C. Mitigation against a single point of failure. Using a multi-cloud strategy distributes workloads across various cloud providers, which reduces the risk associated with outages or security breaches in any one provider. This diversification ensures that a failure or compromise in one cloud environment doesn't jeopardize the entire infrastructure.

Option A is incorrect. Multi-cloud strategies can sometimes complicate management due to the need to interface with different platforms and providers. Centralization isn't the primary benefit in this context.

Option B is incorrect. While encryption is crucial, adopting a multi-cloud approach doesn't automatically encrypt data in transit between different cloud environments. This would require specific configurations and solutions.

Option D is incorrect. While cost optimization can be a factor in adopting a multi-cloud strategy, the primary security advantage is not related to cost reduction.

Question 307. GlobalBank has implemented a backup strategy where only the changes made since the last full backup are

recorded. Considering the need to optimize storage and reduce backup times, the IT team performs this type of backup every day. What backup frequency and type is GlobalBank utilizing?

- (A) **Incremental Backup daily**
- (B) Differential Backup weekly
- (C) Full Backup bi-weekly
- (D) Snapshot Backup daily

Explanation 307. Correct Answer: A. Incremental Backup daily. GlobalBank captures only the changes made since the last full backup, which is characteristic of incremental backups. Furthermore, they perform this type of backup every day, indicating a daily frequency.

Option B is incorrect. Differential backups capture the changes made since the last full backup but would cumulatively grow in size each time until the next full backup, unlike the incremental which resets with each backup.

Option C is incorrect. A full backup would involve backing up all the data, regardless of changes, and the scenario does not mention a bi-weekly frequency.

Option D is incorrect. Snapshot backups capture the state of a system at a particular point in time, but the scenario specifically mentions capturing changes since the last full backup.

Question 308. A defense contractor is working on a new missile system. While the detailed schematics and operational details are classified, they have an overview document that only a select group of partners and stakeholders can view. How should

this overview document be classified?

- (A) Public
- (B) **Restricted**
- (C) Confidential
- (D) Top Secret

Explanation 308. Correct Answer: B. Restricted.

“Restricted” classification is used when access to the document or data needs to be limited to a particular group of individuals. In this scenario, only a select group of partners and stakeholders are allowed to view the overview document, making “Restricted” the most appropriate classification.

Option A is incorrect. “Public” classification would allow anyone to access the document, which is not suitable for this scenario.

Option C is incorrect. While “Confidential” classification would provide a level of protection, it doesn’t specifically restrict access to a defined group as “Restricted” does.

Option D is incorrect. “Top Secret” is a high-level classification that would be more appropriate for the detailed schematics and operational details rather than an overview document.

Question 309. A tech startup is developing a mobile application that offers exclusive content only to users within a specific country due to licensing agreements. Which method should the startup use to ensure that only users within that country can access the content?

- (A) Integrate a time-based one-time password (TOTP) system
- (B) Use geolocation-based access controls
- (C) Enable biometric authentication
- (D) Implement IP whitelisting

Explanation 309. Correct Answer: B. Use geolocation-based access controls. Geolocation-based access controls can identify a user's geographic location and allow or deny access based on predefined geographic boundaries, making it the most suitable solution for the startup's requirement.

Option A is incorrect. TOTP systems provide a second factor of authentication based on time, not geographic location.

Option C is incorrect. Biometric authentication verifies the identity of a user based on physical or behavioral characteristics but does not restrict access based on geography.

Option D is incorrect. IP whitelisting allows access only to specific IP addresses. While it can offer a level of geographic restriction, it's not as precise as geolocation-based controls and may inadvertently block or allow users.

Question 310. MetroTech recently experienced an incident where an employee mistakenly deleted a portion of their database. The IT team was able to restore the data using a backup snapshot taken 24 hours prior. However, some data loss still occurred. Which of the following recommendations would minimize data loss in a similar situation in the future?

- (A) Configure backup snapshots to be taken on a weekly

basis

- (B) Employ a differential backup solution in addition to snapshots
- (C) Increase the storage capacity for backups
- (D) **Use an hourly snapshot backup schedule**

Explanation 310. Correct Answer: D. Use an hourly snapshot backup schedule. Increasing the frequency of snapshot backups, such as taking them every hour, will ensure that the maximum amount of data that can be lost is limited to that hour's worth. This minimizes the potential for data loss compared to a 24-hour window.

Option A is incorrect. Taking weekly snapshots would actually increase the potential data loss window, not decrease it.

Option B is incorrect. While differential backups capture data changes since the last full backup, they don't necessarily reduce the time window for potential data loss like increasing snapshot frequency would.

Option C is incorrect. Increasing storage capacity allows for more backups or longer retention but does not in itself reduce the time window for potential data loss.

CHAPTER 4

SECURITY OPERATIONS

Questions 311-460

Question 311. A financial institution is shutting down one of its data centers. Given the highly sensitive nature of the data stored, the company wants to ensure that there is no possibility of data retrieval from the storage devices. Which of the following methods would be the MOST effective in guaranteeing the destruction of data?

- (A) Overwriting with zeros
- (B) Standard Disk Format
- (C) Physical Destruction
- (D) Running a Disk Cleanup utility

Question 312. A financial application allows users to transfer money to other accounts by entering the account number and the amount to transfer. During a security audit, it was observed that malicious users could enter SQL code into the account number field to manipulate the application's database. Which security technique should the development team implement to address this vulnerability?

- (A) Code obfuscation
- (B) Input validation
- (C) Encryption at rest
- (D) Session timeout

Question 313. After a series of cyberattacks, BetaTech, a financial institution, decided to standardize the configurations across its entire server fleet. They've established a secure baseline configuration for their servers. What should be the NEXT step in ensuring the servers conform to this new baseline?

- (A) Frequently conduct vulnerability scanning on all servers
- (B) Introduce biometric authentication for server access
- (C) Deploy the secure baseline across all servers
- (D) Monitor network traffic to detect anomalies

Question 314. An energy company is looking to enhance the security of its ICS/SCADA systems. They have realized that default configurations might have vulnerabilities. Which of the following is the BEST initial step to take in securing their ICS/SCADA systems?

- (A) Connect the ICS/SCADA systems to the internet for remote monitoring
- (B) Use commercial off-the-shelf software to add a layer of security
- (C) Implement a secure baseline configuration tailored to the ICS/SCADA environment
- (D) Increase the number of users with administrative privileges to ensure rapid response to issues

Question 315. A multinational company is planning to issue company-owned mobile devices to its executives. Given the sensitivity of the data the executives handle, what hardening measure would be MOST effective to ensure the security of these mobile devices?

- (A) Regularly updating the company's social media profiles

to mention the security measures taken

- (B) Implementing biometric authentication in addition to strong passcodes
- (C) Turning off Bluetooth and Wi-Fi when not in use
- (D) Setting the devices to display brighter screen colors

Question 316. A large e-commerce company wants to ensure that their newly developed application is free from any code vulnerabilities before it is deployed to the production environment. They want to catch any software flaws, especially those that might lead to potential security risks. Which of the following methodologies should they employ?

- (A) Runtime application self-protection (RASP)
- (B) Penetration testing on the live application
- (C) Static code analysis
- (D) User acceptance testing (UAT)

Question 317. Jenny, the new CIO of a multinational firm, wants to ensure that every software and hardware asset in the organization has a clearly defined owner responsible for its security and maintenance. Which of the following is the MOST effective way to achieve this?

- (A) Deploy an automated asset discovery tool and assign assets to departments based on their location
- (B) Mandate that every department head is the default owner of all assets within their department
- (C) Conduct regular audits and require individual users to claim ownership of their assets
- (D) Introduce an Asset Management System where assets are logged with defined ownership as they are procured or assigned

Question 318. An audit report indicates that several network switches in a data center lack security configurations, making them potential targets for attackers. Which of the following hardening techniques would BEST reduce the risk associated with these switches?

- (A) Configuring port mirroring to monitor network traffic
- (B) Disabling unused switch ports
- (C) Implementing load balancing across the switches
- (D) Increasing the MAC address table size for performance

Question 319. DeltaSoft has released a new web application. The security team is tasked with observing the application's behavior and responses when it is running to identify potential vulnerabilities. Which method is most appropriate for this purpose?

- (A) Static Analysis
- (B) Fuzz Testing
- (C) Whitebox Testing
- (D) Dynamic Analysis

Question 320. A security analyst at ZetaTech is looking to gather information about emerging threats and vulnerabilities relevant to their industry. Which of the following would be the MOST suitable method to obtain real-time, continuously updated data on potential security issues?

- (A) Relying solely on automated internal vulnerability scanners
- (B) Periodic manual penetration testing
- (C) Subscribing to an OSINT threat feed
- (D) Regularly checking the company's firewall logs

Question 321. A medium-sized enterprise is preparing to upgrade its office workstations. The IT department is considering purchasing devices from a lesser-known, but cheaper, vendor. Which of the following should be the PRIMARY consideration before finalizing the acquisition?

- (A) Whether the vendor offers a longer warranty period
- (B) The aesthetics and design of the workstations
- (C) The vendor's adherence to industry security standards and practices
- (D) The amount of training required for IT staff to support the new devices

Question 322. ClearView Industries wants to give their employees the flexibility to choose their own devices for work while retaining control over the device configurations and applications. Which deployment model would be the MOST appropriate for ClearView's objectives?

- (A) Bring Your Own Device (BYOD)
- (B) Choose Your Own Device (CYOD)
- (C) Corporate-owned, Personally Enabled (COPE)
- (D) Fixed Device Deployment (FDD)

Question 323. A recently hired security analyst at CyberTech Inc. wants to get a better understanding of the organization's network infrastructure. Which of the following activities would provide a LIST of servers, workstations, printers, switches, and routers currently active in the network?

- (A) Vulnerability Scanning
- (B) Intrusion Detection
- (C) Network Enumeration
- (D) Penetration Testing

Question 324. A network engineer is preparing a new batch of routers for deployment in a large organization. Which of the following steps should the engineer prioritize to ensure that the routers are securely configured from the start?

- (A) Configure the routers to use DHCP to dynamically assign IP addresses to connected devices
- (B) Change the default administrative credentials on the routers
- (C) Update the routers' firmware to the latest, most feature-rich version, regardless of its security posture
- (D) Customize the routers' LED colors for easy identification in the server room

Question 325. A university is looking to revamp its wireless network to provide secure access for students and faculty. The IT department wants an authentication method that leverages a centralized server to validate user credentials and can integrate with their existing directory service. Which authentication protocol should they consider?

- (A) Pre-shared Key (PSK)
- (B) Lightweight Extensible Authentication Protocol (LEAP)
- (C) Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- (D) Shared Secret Challenge

Question 326. TechHive Corp. is planning to sell some of its old servers. Before selling, they want to ensure that no retrievable personal or business data remains on the hard drives. Which of the following methods should TechHive use to ensure the drives are clean and the data cannot be recovered?

- (A) Simple Format

- (B) Magnetic Wiping
- (C) Physical Destruction
- (D) Standard Defragmentation

Question 327. The network administrator of a rapidly growing tech firm is concerned about the potential vulnerabilities of the company's switches. Which of the following measures is MOST effective in hardening these network switches against possible attacks?

- (A) Assigning static IP addresses to all connected devices
- (B) Implementing strong password policies for switch access
- (C) Upgrading the switches to support 10Gbps for future expansion
- (D) Customizing the switch LED colors for easy identification

Question 328. A robotics company is developing an autonomous vehicle that relies on a Real-Time Operating System (RTOS) to manage its operations. The development team wants to ensure that the vehicle's RTOS has a solid security posture. What should the team prioritize when establishing a secure baseline for this RTOS?

- (A) Installing a robust antivirus software
- (B) Enabling all features for maximum functionality
- (C) Regularly backing up the RTOS data to the cloud
- (D) Minimizing the number of services and open ports

Question 329. After deploying wireless access points in a large manufacturing facility, employees report inconsistent wireless connectivity in some areas. What tool would be most effective

for the IT team to use to visualize areas of weak wireless signal strength?

- (A) Network bandwidth monitor
- (B) Protocol analyzer
- (C) Heat map software
- (D) Intrusion detection system

Question 330. Sarah, an end-user, downloads a software update from a website. Before installing, she wants to make sure the software hasn't been modified maliciously and that it originates from a trusted source. What should Sarah check to validate this?

- (A) The SSL certificate of the website
- (B) The application's code signing certificate
- (C) The application's open-source repositories
- (D) The software's user reviews

Question 331. A local coffee shop offers free Wi-Fi to its customers. Recently, there have been reports of man-in-the-middle attacks on the network. The owner decides to upgrade the wireless security and wants to implement a cryptographic protocol to secure data transmissions. Which protocol would provide a balance between security and performance for the public Wi-Fi users?

- (A) Advanced Encryption Standard (AES)
- (B) Wired Equivalent Privacy (WEP)
- (C) RC4 Stream Cipher
- (D) Open Wireless

Question 332. A software development company has decided to host their applications in a multi-cloud environment. Before deploying, they are looking to enhance the security of their

cloud-based resources. Which of the following is the BEST practice for hardening their cloud infrastructure?

- (A) Ensure that all cloud storage buckets or containers are publicly accessible for easier data sharing
- (B) Apply consistent security configurations and policies across all cloud providers
- (C) Use the same SSH key pairs across all cloud instances for uniformity
- (D) Limit the use of Identity and Access Management (IAM) roles to senior staff only

Question 333. After running a vulnerability scan on the company's infrastructure, a security analyst notices a reported vulnerability on a server. However, after manual verification, the analyst determines that the vulnerability doesn't actually exist on the server. What is this situation best described as?

- (A) A false negative
- (B) A true positive
- (C) A false positive
- (D) A confirmation bias

Question 334. An e-commerce platform recently suffered a data breach where attackers exploited cookies to impersonate user sessions. A security analyst is tasked with recommending measures to secure user cookies. Which of the following measures will ensure that cookies are transmitted securely between the user's browser and the server?

- (A) Storing cookies in the database
- (B) Implementing the "Secure" attribute for cookies
- (C) Increasing the cookie expiration time
- (D) Base64 encoding the cookie content

Question 335. A security analyst is reviewing a vulnerability report and sees a reference to CVE-2023-12345 with a CVSS score of 9.5. Which of the following conclusions can the analyst draw based on this information?

- (A) The vulnerability was first identified in the year 2023
- (B) The vulnerability is of low severity
- (C) The vulnerability affects only software produced in 2023
- (D) CVE-2023-12345 is the software vendor's internal code for the vulnerability

Question 336. AlphaTech is seeking a comprehensive source of intelligence about the latest cyber threats targeting its specific industry. While OSINT provides valuable data, the company is considering investing in a more specialized solution. Which of the following would best address AlphaTech's needs?

- (A) Implementing internal honeypots to trap attackers
- (B) Subscribing to a third-party threat intelligence feed
- (C) Regularly attending cyber security conferences
- (D) Using open-source vulnerability scanners

Question 337. ABC Corp recently adopted a Bring Your Own Device (BYOD) policy. The IT department is concerned about the potential risks associated with personal devices accessing the corporate network. Which of the following solutions would be MOST effective for enforcing security policies on these personal mobile devices?

- (A) Installing antivirus software on each device
- (B) Establishing a separate guest Wi-Fi network for mobile devices
- (C) Using Mobile Device Management (MDM) to enforce

security policies

(D) Mandating that employees use strong passwords on their personal devices

Question 338. David, an IT administrator, noticed an unusually high data usage on several company-owned mobile devices even when they are connected to the corporate Wi-Fi. He suspects these devices might be using cellular data in the background. Which of the following solutions should David implement to ensure that company devices use only the corporate Wi-Fi for data transactions when they're in the office?

(A) Enable Airplane mode on all devices

(B) Set up a Wi-Fi whitelist

(C) Implement a mobile device management (MDM) policy to prioritize Wi-Fi

(D) Disable cellular antennas in the office area

Question 339. A security team recently upgraded their intrusion detection system (IDS). Since the upgrade, the system hasn't flagged any intrusions, even though intrusion attempts are a regular occurrence. What is this situation best characterized as?

(A) A true negative

(B) A false negative

(C) A true positive

(D) A confirmation feedback

Question 340. XYZ Corporation is planning to deploy a new wireless infrastructure in their newly acquired office building. The IT manager wants to ensure optimal wireless coverage throughout the premises. Which of the following should the IT team prioritize before installing the wireless access points?

- (A) Purchase the most expensive wireless access points to ensure maximum range
- (B) Conduct a site survey to determine the best locations for access points
- (C) Deploy all access points near windows to enhance signal strength
- (D) Ensure all users have 5GHz capable devices

Question 341. XYZ Company uses MDM to manage company-owned and employee-owned mobile devices. An employee reported losing their personal phone over the weekend. What MDM feature should the IT department use to ensure that sensitive company data on the lost phone isn't accessed?

- (A) Monitor the device's location
- (B) Force update the device's apps
- (C) Remote wipe the device
- (D) Change the user's email password

Question 342. After a series of cyber incidents, AlphaTech Corp. wants to take proactive measures to identify vulnerabilities in their network. They aim to obtain a comprehensive report of potential weaknesses without exploiting them. Which of the following would best meet this objective?

- (A) Penetration test
- (B) Vulnerability scan
- (C) Red team assessment
- (D) Port security

Question 343. GammaTech is in the final stages of deploying a new application. Before the deployment, the security team

wants to examine the application's code without executing it to identify any potential vulnerabilities. Which vulnerability identification method should the team employ?

- (A) Penetration Testing
- (B) Dynamic Analysis
- (C) Static Analysis
- (D) Fuzz Testing

Question 344. During a routine vulnerability assessment, TechInc discovers a weakness in their system that, if exploited, would allow an attacker to modify existing user accounts, including privileges. Which classification best describes this vulnerability?

- (A) Elevation of privilege vulnerability
- (B) Disclosure vulnerability
- (C) Replay vulnerability
- (D) Remote code execution vulnerability

Question 345. A healthcare organization uses embedded systems in various medical devices. They are aware of the potential threats these systems can pose if not properly secured. Which of the following is NOT a recommended practice when hardening embedded systems in this context?

- (A) Regularly patching and updating the firmware of the devices
- (B) Allowing unrestricted access to the devices for ease of use by the medical staff
- (C) Disabling unnecessary services and features not required for the device's primary function
- (D) Changing default credentials and using strong, unique passwords for device access

Question 346. TechSoft Corp. is implementing a new asset-tracking system to monitor its vast array of computing resources. Which of the following should be the PRIMARY reason for maintaining an up-to-date hardware and software inventory?

- (A) To ensure software licenses are renewed on time
- (B) To identify and respond to unauthorized devices or software promptly
- (C) To aid in the procurement of new hardware and software
- (D) To provide employees with an understanding of available resources

Question 347. An enterprise is deploying IoT-based security cameras across multiple office locations. As the lead security professional, what recommendation would you prioritize to establish a secure baseline for these devices?

- (A) Setting the devices to public mode so all employees can access the feed for transparency
- (B) Regularly updating the device firmware to patch known vulnerabilities
- (C) Enabling Universal Plug and Play (UPnP) to ensure easy connectivity for all devices on the network
- (D) Using the same password for all cameras for ease of management

Question 348. A medium-sized enterprise is concerned about the security of its office workstations after a series of malware infections. As a security analyst, which of the following recommendations would BEST improve the security baseline of the workstations?

- (A) Install multiple antivirus solutions to ensure maximum

detection

- (B) Set up screensavers with cyber hygiene tips to educate users
- (C) Disable unnecessary services and ports on the workstations
- (D) Frequently change the desktop wallpaper to prevent monotony

Question 349. AlphaCorp is migrating to cloud infrastructure and wants to ensure all virtual machines (VMs) are securely configured from the onset. Before deploying multiple VM instances, what should AlphaCorp do to ensure each VM starts from a secure configuration?

- (A) Use the default VM templates provided by the cloud provider
- (B) Establish a secure baseline for VM configurations and use it for deployment
- (C) Regularly backup all VMs
- (D) Use multi-factor authentication for cloud access

Question 350. A multinational company is deploying a new set of servers in its data centers across various countries. Which of the following steps should be taken FIRST to ensure the servers are secured against potential threats?

- (A) Set up a monitoring system to alert the IT team of any irregular activities
- (B) Deploy all the software applications the company might need in the future
- (C) Use the server's default configuration to ensure manufacturer's best practices are maintained
- (D) Disable any unused services and ports on the server

Question 351. While analyzing a vulnerability in a company's web application, the security team refers to a specific CVE to understand the vulnerability's details. They further assess its CVSS score to decide on the remediation urgency. Which of the following best describes the purpose of the CVE and CVSS in this context?

- (A) CVE provides a severity score, while CVSS gives a unique identifier for the vulnerability
- (B) CVE and CVSS both offer a scoring mechanism to rank vulnerabilities
- (C) CVE provides a unique identifier, while CVSS offers a standardized severity score
- (D) CVE and CVSS are regulatory requirements for all software applications

Question 352. The network administrator at a university wants to ensure that when students log onto the campus wireless network, their credentials are verified by the university's central authentication server. Additionally, the administrator wants to make sure that the data between the wireless access point and the central server is encrypted. Which solution should the administrator implement?

- (A) WPA3 with SAE
- (B) WPA2-Personal with AES
- (C) WPA2-Enterprise with RADIUS
- (D) Open wireless with VPN

Question 353. As part of the company's vulnerability management initiative, the security team has decided to conduct a series of penetration tests. Which of the following is the PRIMARY reason for incorporating penetration testing as a

threat identification method?

- (A) To ensure compliance with regulatory requirements
- (B) To validate the efficiency of security awareness training
- (C) To actively exploit vulnerabilities and assess potential impact
- (D) To identify misconfigurations in the SIEM system

Question 354. An organization has recently received a new software patch for its critical infrastructure. Before deploying it to production, the security team wants to understand its behavior and ensure it doesn't contain any malicious code. Which of the following methods would be MOST effective for safely executing and observing the patch's behavior?

- (A) Deploying the patch during a maintenance window
- (B) Running the patch within a sandbox environment
- (C) Conducting a code review of the patch
- (D) Installing the patch on a virtual machine

Question 355. GreenTech Inc. is selling a set of old servers to another company. Before the transaction, they want to ensure the data on these servers is irretrievable and they can prove that due diligence was performed. What should GreenTech seek to assure the buyer of proper data destruction?

- (A) A receipt of sale for the servers
- (B) A detailed log of the server's usage
- (C) A certificate of data sanitization
- (D) A user manual of the servers

Question 356. Jane, the CISO at a financial institution, is overseeing the decommissioning of several old servers. She is aware that while some data must be destroyed, other data must

be retained due to industry regulations. Which principle should Jane primarily focus on to ensure compliance?

- (A) Minimum necessary principle
- (B) Principle of least privilege
- (C) Data retention policy
- (D) Mandatory vacation policy

Question 357. CyberFirm, a leading software development company, recently updated their server OS due to new features and patches. Given that they have already established and deployed a secure baseline in the past, what should CyberFirm do NEXT to ensure continued security?

- (A) Conduct a complete system reboot for all servers
- (B) Re-deploy the same baseline without any modifications
- (C) Update the secure baseline to include new configurations and then deploy it
- (D) Implement a new firewall rule for the servers

Question 358. MatrixCorp recently adopted a mobile strategy where employees are provided with company-owned devices. These devices are also allowed for personal use, but the organization retains the ability to manage and monitor them. Which deployment model is MatrixCorp using?

- (A) Bring Your Own Device (BYOD)
- (B) Choose Your Own Device (CYOD)
- (C) Corporate-owned, Personally Enabled (COPE)
- (D) Public Device Deployment (PDD)

Question 359. A company has recently upgraded its wireless infrastructure and wants to ensure that the data transmitted over its wireless network is protected using the most recent and

secure encryption standards. Which of the following should the company configure on its wireless access points?

- (A) WEP
- (B) WPA
- (C) WPA2
- (D) WPA3

Question 360. A security analyst is exploring ways to proactively identify vulnerabilities within the organization's infrastructure. Which of the following provides the BEST method for the analyst to receive real-time threat intelligence from the dark web?

- (A) Utilizing a vulnerability scanner on the organization's internal network
- (B) Subscribing to a dark web threat intelligence feed
- (C) Conducting regular penetration tests on external-facing systems
- (D) Reviewing daily reports from the organization's SIEM system

Question 361. XYZ Corp is designing their new web application infrastructure. They want to ensure that all web traffic to and from their application is encrypted. In addition to selecting HTTPS as the protocol, which default port should they configure for this encrypted traffic?

- (A) 21
- (B) 80
- (C) 443
- (D) 25

Question 362. TechWorld Corp is concerned about cybercriminals sending emails that appear to come from its domain to deceive its clients. The company wants to implement a solution that would allow receiving email servers to validate that an email claiming to come from TechWorld Corp's domain indeed originates from an approved server. Which of the following should the company implement?

- (A) SMTP authentication
- (B) DKIM
- (C) POP3 over SSL
- (D) S/MIME

Question 363. After a security incident, a forensic investigation revealed that a compromised internal workstation was communicating with a known malicious IP address. To prevent further communication, the security team decided to take immediate action. Which of the following is the BEST immediate action to ensure the workstation cannot communicate with that IP?

- (A) Implement a block rule on the web filter for the IP address
- (B) Disable the network port of the compromised workstation
- (C) Use a honeypot to divert the traffic from the malicious
- (D) Update the firewall's firmware

Question 364. Amy, a network administrator, is researching tools to assist with automating the evaluation of her organization's systems against a specific security baseline. She comes across SCAP and wants to implement it. Which of the following BEST describes the primary function of the Security

Content Automation Protocol (SCAP)?

- (A) To facilitate the real-time transfer of threat intelligence feeds
- (B) To provide an interface for user authentication against Active Directory
- (C) To allow for automated vulnerability management and policy compliance evaluation
- (D) To offer encrypted communication channels for remote system management

Question 365. A pharmaceutical company is working on a new drug formula that promises to revolutionize the treatment of a particular disease. The R&D team has detailed documentation on the components, procedures, and results of the drug trials. How should this documentation be classified to ensure that only the right people within the company have access?

- (A) Implement a Domain Name System (DNS) firewall
- (B) Employ URL scanning to identify and block malicious URLs
- (C) Rely on manual reporting of suspicious URLs by employees
- (D) Use a Virtual Private Network (VPN) to redirect all employee web traffic

Question 366. A financial institution wants to ensure that any unauthorized access to customer data triggers an immediate alert to the security team. Which of the following approaches would be the MOST effective in achieving this requirement?

- (A) Configure alerts for any modification to database records
- (B) Set up alerts for successful logins during off-business

hours

- (C) Establish alerting thresholds based on anomalous user behavior
- (D) Send daily reports of all access attempts to the security team for review

Question 367. A marketing team is collaborating on a new campaign and requires access to a shared folder. However, they shouldn't be able to modify files created by others. How should permissions be set on this shared folder?

- (A) Assign the marketing team full control
- (B) Allow the marketing team read-only access
- (C) Assign the marketing team write-only access
- (D) Assign the marketing team modify permission but deny the delete permission

Question 368. Alice, a cybersecurity analyst, is tasked with identifying potential weaknesses in a newly deployed web application's infrastructure before it goes live. She wants a tool that can proactively discover and report on system vulnerabilities, missing patches, and misconfigurations. Which of the following should Alice utilize for this purpose?

- (A) Intrusion Detection System (IDS)
- (B) Network sniffer
- (C) Vulnerability scanner
- (D) Security Information and Event Management (SIEM) system

Question 369. Globex Industries is expanding its data centers across multiple geographic locations. The IT team wants to have a centralized system to get real-time status, outages, and metrics

of all data center infrastructures. Which of the following solutions would be the MOST effective for this purpose?

- (A) Data Loss Prevention (DLP) tools
- (B) Distributed Denial of Service (DDoS) protection
- (C) Security Information and Event Management (SIEM)
- (D) Infrastructure Management Platform (IMP)

Question 370. The IT department of XYZ Corp is keen on preventing users from changing specific system settings, such as altering the firewall configurations. The majority of their infrastructure is based on Windows operating systems. Which of the following would be the most effective way to achieve this?

- (A) Use SELinux to enforce strict access controls
- (B) Utilize Group Policy to set and enforce policies related to system settings
- (C) Deploy a third-party software solution to lock system settings
- (D) Implement a user training program to guide users on system settings best practices

Question 371. A company plans to upgrade its email server to ensure that email transmission between their mail server and client applications is encrypted. Which of the following protocols would be the most appropriate for this purpose?

- (A) HTTP
- (B) FTP
- (C) IMAP over SSL/TLS
- (D) SNMP

Question 372. Lisa, a security administrator, is using a popular benchmark to ensure the web servers in her organization are

configured securely. She wants to make sure that unnecessary services are disabled, and appropriate permissions are set. Which of the following organizations is MOST likely the source of the benchmark she is using?

- (A) PCI DSS
- (B) OWASP
- (C) CIS
- (D) GDPR

Question 373. The IT department at TechCorp Ltd has been instructed to ensure that critical system files remain unchanged to avoid potential security breaches. They want to implement a system that can provide alerts whenever there is an unauthorized change to these files. Which of the following would best serve this purpose?

- (A) Data Loss Prevention (DLP)
- (B) Intrusion Detection System (IDS)
- (C) File Integrity Monitoring (FIM)
- (D) Remote Monitoring and Management (RMM)

Question 374. ABC Tech has a mixed environment with both Linux and Windows servers. They want to ensure that processes running on their Linux servers only have access to specific resources and are restricted from performing certain actions. Which of the following tools would be most appropriate for this task?

- (A) Use Group Policy on their Windows servers and apply it to Linux servers
- (B) Implement a strict user training regimen to inform users about security best practices
- (C) Enable Security-Enhanced Linux (SELinux) in

enforcing mode

(D) Limit user access to Linux servers

Question 375. Sarah, a security administrator, is implementing a monitoring solution for her organization's server infrastructure. She wants a solution that does not require any additional software to be installed on the servers themselves. Which type of monitoring approach should Sarah choose?

(A) Agent-based monitoring

(B) Intrusion Detection System (IDS)

(C) Agentless monitoring

(D) Network-based Application Performance Monitoring (APM)

Question 376. PharmaCorp, a pharmaceutical company, wants to ensure that its researchers cannot transfer proprietary formulas and research data to external storage devices or cloud storage. The company needs a solution to prevent such transfers while allowing other types of data to be transferred. What should they implement?

(A) Web Application Firewall (WAF)

(B) Data Encryption Tool

(C) Data Loss Prevention (DLP)

(D) Virtual Private Network (VPN)

Question 377. CyberFirm has been facing issues with phishing campaigns where attackers spoof their domain to send fraudulent emails. They already implemented DKIM to sign their emails but want an additional measure to specify which mail servers are authorized to send emails on behalf of their domain. Which security measure should CyberFirm adopt?

- (A) SPF
- (B) PGP
- (C) SSL certificate
- (D) IMAP

Question 378. A school wants to prevent its students from accessing inappropriate websites during class hours. The IT department decides to implement a solution that blocks requests to specific domain names associated with inappropriate content. Which of the following security solutions would best address this need?

- (A) Firewall filtering based on IP addresses
- (B) Intrusion Detection System monitoring
- (C) Virtual Private Network (VPN) enforcement
- (D) DNS filtering with a blacklist

Question 379. A large financial institution recently experienced a security breach where an attacker was able to bypass its intrusion detection system (IDS). Upon investigation, the security team found out that the attacker utilized a zero-day exploit. In the aftermath, what should the institution do to enhance the capability of its IDS?

- (A) Switch from a signature-based IDS to a behavior-based IDS
- (B) Disable the IDS and rely solely on firewall rules
- (C) Update the IDS with the latest threat intelligence feeds and signatures
- (D) Reduce the frequency of IDS signature updates

Question 380. A security analyst at CyberSecure Corp. reviews a vulnerability report concerning an application that could allow

attackers to upload malicious scripts. Once these scripts are executed, they can grant attackers complete control over the application. How should this vulnerability be primarily classified?

- (A) Integrity vulnerability
- (B) Availability vulnerability
- (C) Remote code execution vulnerability
- (D) Disclosure vulnerability

Question 381. After a recent security incident in the organization, the IT team noticed that several legitimate activities were being flagged by the intrusion detection system, resulting in a high number of false positives. What is the MOST appropriate action to improve the system's accuracy and reduce unnecessary alerts?

- (A) Disable the intrusion detection system for a week to observe regular network traffic patterns
- (B) Set up a stricter firewall rule to block all external traffic
- (C) Implement alert tuning to refine the system's detection criteria
- (D) Encourage employees to reduce their internet usage

Question 382. ABC Corp has recently faced a security breach due to a contractor connecting an infected laptop to the corporate network. Management wants to implement a solution that would ensure that any device connecting to the corporate network meets the company's security standards, including up-to-date antivirus definitions. Which solution should ABC Corp consider?

- (A) Intrusion Detection System (IDS)
- (B) Virtual Private Network (VPN)

- (C) Network Access Control (NAC)
- (D) Web Application Firewall (WAF)

Question 383. Global Corp received a report that some of its customers received phishing emails that seemed to originate from the company's domain. The IT team checked and confirmed that SPF and DKIM configurations were correctly set. What additional email security measure can Global Corp implement to provide clear policies on how the emails should be treated if they don't align with SPF and DKIM?

- (A) Enabling TLS encryption
- (B) Implementing DMARC policies
- (C) Setting up a new SMTP server
- (D) Increasing email retention period

Question 384. A financial firm has just experienced a cyber attack, and the IT team identified a piece of malware that evaded their traditional antivirus solutions. The CISO now wants to not only detect but also be able to analyze and respond to such advanced threats in real-time. Which solution should the firm consider implementing?

- (A) Vulnerability Scanner
- (B) Intrusion Prevention System (IPS)
- (C) Endpoint Detection and Response (EDR)
- (D) Patch Management System

Question 385. After the recent cyber-attack on Acme Corp, the IT security team decided to enhance their proactive defense mechanism. They want to start with identifying unpatched and vulnerable systems on their network. Which of the following scanning activities would BEST assist them in this endeavor?

- (A) Conducting a passive scan during business hours
- (B) Implementing a full open port scan on all systems
- (C) Running a credentialed vulnerability scan on their network
- (D) Scanning the external perimeter for domain name resolutions

Question 386. A software developer in a company notices that a legitimate software tool they use is repeatedly flagged and quarantined by the company's security solution. Which of the following is the BEST action the cybersecurity team can take to address this without compromising security?

- (A) Turn off the antivirus solution
- (B) Whitelist the software tool in the antivirus settings
- (C) Decrease the security level of the antivirus
- (D) Install a different antivirus solution

Question 387. AlphaTech, a growing SaaS company, has multiple applications deployed across different cloud providers. The security team struggles to manage and analyze logs from these disparate sources. Which solution would BEST help AlphaTech centralize their logs for a more streamlined analysis?

- (A) Network Intrusion Detection System (NIDS)
- (B) Log Aggregation Tool
- (C) Data Loss Prevention (DLP) software
- (D) Vulnerability Scanner

Question 388. BetaTech, a tech manufacturing firm, wants to ensure that a potential compromise of its IoT devices will not endanger its primary manufacturing control systems. Which of the following approaches would be most effective in achieving

this?

- (A) Using a single robust firewall for the entire network
- (B) Periodic password changes for IoT devices
- (C) Segmenting the IoT devices from the manufacturing control systems
- (D) Enabling automatic updates for all IoT devices

Question 389. A global manufacturing company wants to ensure its employees worldwide do not access websites promoting hate speech, gambling, or explicit content during working hours. To meet this requirement, which web filtering technique would be the most efficient?

- (A) Deploy a centralized proxy with location-based filtering
- (B) Use a blacklist of specific URLs known to contain such content
- (C) Implement content categorization and block undesired categories
- (D) Monitor internet usage logs and reprimand violators

Question 390. TechCo, a medium-sized enterprise, is planning to implement a solution to monitor, control, and restrict web access for its employees to improve productivity and enhance security. They also want to cache frequently accessed web content to reduce bandwidth consumption. Which solution would BEST fit TechCo's requirements?

- (A) Deploy a decentralized proxy on each departmental network
- (B) Set up a DNS-based filtering service
- (C) Use a centralized proxy with caching capabilities
- (D) Recommend browser extensions for web filtering to all employees

Question 391. An organization is planning to deploy a new web application that will be accessible from both the internal network and the internet. The application will communicate exclusively over HTTPS. The security administrator is asked to configure the firewall to allow the necessary traffic. Which of the following should the administrator configure?

- (A) Allow port 21 and block all others
- (B) Allow port 443 and block all others
- (C) Allow port 80 and block all others
- (D) Allow port 23 and block all others

Question 392. The company's security administrator observes that there are multiple unauthorized access attempts originating from IP addresses in a specific range. The administrator wants to prevent these IP addresses from accessing the corporate network temporarily. Which of the following firewall configurations would BEST address this requirement?

- (A) Configure an implicit deny rule for the specific IP range
- (B) Set up a honeypot for the specific IP range
- (C) Allow the IP range but set a bandwidth limit
- (D) Add the IP range to a whitelist

Question 393. The IT department of Globex Corp is concerned about the increasing number of malicious websites being accessed from company laptops while employees are working remotely. They want to ensure that the web filter policies set in the corporate network are enforced even when devices are offsite. What would be the BEST solution to address this concern?

- (A) Implement a cloud-based web filtering solution
- (B) Use a VPN to force all remote traffic through the

corporate network

- (C) Deploy an agent-based web filter on all company laptops
- (D) Periodically send reminders to employees about acceptable web usage

Question 394. Lisa, a cybersecurity analyst, is setting up a centralized system to correlate logs from multiple sources, detect malicious activities in real-time, and produce comprehensive security reports. Which tool should Lisa consider for this purpose?

- (A) Network Intrusion Detection System (NIDS)
- (B) Web Application Firewall (WAF)
- (C) Vulnerability Scanner
- (D) Security Information and Event Management (SIEM)

Question 395. Lucy, the IT security manager of a financial company, receives an automated alert that an employee attempted to email a document containing social security numbers to an external email address. Which of the following tools most likely generated this alert?

- (A) Network Intrusion Detection System (NIDS)
- (B) Data Loss Prevention (DLP) solution
- (C) Vulnerability Scanner
- (D) Packet Analyzer

Question 396. An online banking platform wants to improve its customer verification process when users open a new account. Which of the following identity proofing methods would be the MOST secure for this purpose?

- (A) Asking users to select a security question and answer

from a list

- (B) Requiring users to upload a photo of a government-issued ID and a selfie
- (C) Sending a verification code to the user's email address
- (D) Prompting users to provide their favorite color

Question 397. A company has recently noticed an increased number of employees accessing social media sites during work hours, leading to decreased productivity. To counter this, the security administrator decides to limit access to these websites during peak working hours. Which firewall rule modification should the administrator make?

- (A) Implement an Intrusion Prevention System (IPS) rule to block social media content
- (B) Change the firewall rule to deny access to known social media IP addresses between 9 AM and 5 PM
- (C) Use the firewall's URL filtering capability to blacklist social media URLs
- (D) Increase the firewall's bandwidth to accommodate the excess traffic

Question 398. A company wants to host a public-facing website but ensure that even if the website gets compromised, attackers cannot gain access to sensitive internal data. Which of the following is the BEST configuration to achieve this?

- (A) Place the web server on the internal network and strictly monitor the traffic
- (B) Place the web server in the DMZ with a firewall in front of it and another firewall between the DMZ and the internal network
- (C) Directly connect the web server to the internet without a

firewall and move sensitive data off the server

(D) Place the web server in the DMZ and connect it directly to the internal network without a firewall

Question 399. A Security Analyst at BetaTech is reviewing the monitoring tools deployed across the organization. She wants to ensure that every tool can detect unauthorized changes made to system files and configurations. Which of the following tools is BEST suited for this purpose?

(A) Network protocol analyzer

(B) File integrity monitoring (FIM) system

(C) Bandwidth monitoring tool

(D) Passive vulnerability scanner

Question 400. A company has noticed an increase in malware infections over the past month. After investigating, it was determined that the infections were caused by employees visiting websites that were newly registered but had malicious intent. Which of the following would be the BEST approach to mitigate this threat?

(A) Implement a block rule to deny access to all websites

(B) Use a web filter that incorporates domain reputation checks and blocks domains registered recently

(C) Set the web filter to block all websites not categorized as "Business"

(D) Enforce multi-factor authentication for all internet-based applications

Question 401. At AlphaTech, the security team is assessing vulnerabilities in a newly deployed cloud infrastructure. While analyzing potential risks, they consider factors such as the

physical location of data centers, local laws and regulations, and natural disaster frequencies. What are these considerations known as in the context of vulnerability management?

- (A) Asset valuation factors
- (B) Risk response variables
- (C) Threat intelligence variables
- (D) Environmental variables

Question 402. Caroline, a security analyst, receives an alert that an unfamiliar file has been detected on a mission-critical server. She suspects it might be malware. What is the BEST immediate action Caroline should take regarding this potential threat?

- (A) Delete the file immediately to prevent further damage
- (B) Quarantine the file to prevent it from executing or spreading
- (C) Make a copy of the file for further analysis
- (D) Notify all employees about the suspicious file

Question 403. Jennifer, an IT administrator, is asked to onboard a new remote employee for a sales role. Which of the following is the BEST approach for provisioning the user account?

- (A) Assign the new user the same access privileges as the CEO because they might require all resources
- (B) Provide the new user with administrative rights to ensure they can install and configure any needed software
- (C) Use the access privileges from a template of a salesperson to provide the required resources
- (D) Allow the new user to decide and self-select the necessary access based on their job role

Question 404. AlphaTech, a leading IT company, recently identified a critical vulnerability in its primary software product. They have developed a patch to address the vulnerability. Before distributing the patch to its customers, which of the following should AlphaTech ideally perform?

- (A) Deploy the patch on all company systems
- (B) Notify the media about the vulnerability
- (C) Test the patch in a controlled environment
- (D) Offer compensation to affected customers

Question 405. After a major security incident, DeltaTech implemented several security patches to address vulnerabilities in their infrastructure. To ensure the effectiveness of these patches, what should be DeltaTech's primary next step?

- (A) Deploy additional firewalls at the network perimeter
- (B) Provide cybersecurity training to all employees
- (C) Rescan the systems to check if vulnerabilities are effectively addressed
- (D) Change all user passwords across the organization

Question 406. An e-commerce company is rolling out a new web application to facilitate online payments. The IT department wants to be immediately notified of any application errors or unauthorized modifications to the application's codebase. Which of the following tools should they implement?

- (A) Web Application Firewall (WAF)
- (B) Application Performance Monitoring (APM)
- (C) Domain Name System (DNS) monitoring tool
- (D) Network flow analyzer

Question 407. Paul, a network administrator, has configured various networking devices in his organization to send alerts in the event of specific failures. After a switch experienced a power supply failure, Paul received an immediate notification. Which of the following did Paul most likely utilize to receive this notification?

- (A) Syslog server
- (B) Simple Network Management Protocol (SNMP) traps
- (C) Packet sniffer
- (D) Firewall logs

Question 408. DeltaCorp, a retail company, has assessed that a security breach might result in a loss of \$1 million in sales. The company has determined that they can tolerate a loss of up to \$500,000, but anything beyond that would severely impact operations. To cover the potential financial loss beyond their tolerance level, they decide to purchase cybersecurity insurance. Which of the following terms best describes the \$500,000 figure?

- (A) Risk appetite
- (B) Risk threshold
- (C) Risk capacity
- (D) Risk assessment

Question 409. Samantha, a security analyst, has been tasked with creating a monthly report for senior management detailing the security posture of the company. Which of the following is the MOST important element to include to ensure the report effectively communicates the company's current security status?

- (A) Detailed technical logs of all security incidents
- (B) Graphical representation of incidents by category

- (C) A complete list of all users and their access levels
- (D) Copies of recent phishing emails for demonstration

Question 410. After a recent security incident, Sarah, a network security analyst, wants to analyze the flow data of network traffic to identify patterns and potential threats. She wants to collect metadata about IP traffic flow and gather details like IP addresses, ports, and protocols used. Which tool should Sarah employ to obtain this information?

- (A) Intrusion Detection System (IDS)
- (B) Syslog server
- (C) NetFlow collector
- (D) Simple Network Management Protocol (SNMP) traps

Question 411. A security analyst has been tasked with investigating a possible data breach. While reviewing the network logs, the analyst noticed an unusual increase in outbound traffic to an unfamiliar IP address during non-business hours. The traffic appears to be encrypted and is associated with a known server containing sensitive data. Which of the following is the MOST likely explanation for this behavior?

- (A) The server is downloading patches
- (B) An employee is accessing the server remotely
- (C) A backup of the server is being performed
- (D) Data exfiltration is occurring

Question 412. ExamsDigest Enterprises wants to streamline their permission assignments. They decide that rather than assigning permissions to each user individually, they will group users based on departmental roles and then assign permissions to these groups. For example, all members of the “Marketing”

role would have access to the marketing database. Which access control method is ExamsDigest Enterprises employing?

- (A) Rule-based access control
- (B) Mandatory Access Control (MAC)
- (C) Discretionary Access Control (DAC)
- (D) Role-Based Access Control (RBAC)

Question 413. BetaTech is implementing a new authentication mechanism for its data center technicians. Instead of using key cards, technicians will now have to look into a device that maps a specific pattern to authenticate their identity. Which of the following is BetaTech likely implementing?

- (A) Password system
- (B) Retina scanning
- (C) Hardware token
- (D) Knowledge-based questions

Question 414. A global financial company experiences sporadic cyber attacks on its infrastructure. The company notices that attacks that occur during non-business hours often result in more significant damage due to delayed responses. Which of the following measures would BEST decrease the reaction time to these off-hour attacks?

- (A) Train the security staff to handle larger volumes of incidents during business hours
- (B) Implement an automated intrusion detection and response system
- (C) Increase the number of security staff during non-business hours
- (D) Send email notifications to security personnel when attacks are detected

Question 415. A digital forensics investigator has just concluded an investigation regarding a potential insider threat. Before presenting the findings to the organization's board, which of the following should the investigator ensure about the forensic report?

- (A) The report includes technical jargon to showcase the depth of the investigation
- (B) The report emphasizes the investigator's credentials and experience
- (C) The report provides a clear, concise summary of findings without unnecessary technical details
- (D) The report contains detailed logs of every action taken by the investigator

Question 416. MegaCorp is transitioning to a cloud-based infrastructure and wants to allow its employees to access multiple cloud services without re-entering their credentials every time. They currently have an on-premises LDAP directory in place. Which approach should MegaCorp take to provide a seamless authentication experience?

- (A) MegaCorp should abandon their LDAP directory and create individual accounts for each cloud service
- (B) Integrate their LDAP with a Single Sign-On (SSO) solution that supports cloud services
- (C) Store passwords in a plaintext file for users to access and login to cloud services manually
- (D) Force users to change passwords every day to enhance security across all cloud platforms

Question 417. At ExamsDigest, employees can access the company's cloud-based storage system. However, access to

certain files within the storage is determined by the employee's department, job title, and years of service. For instance, senior managers in the finance department with more than five years of service can view the company's financial forecasts. Which access control model is ExamsDigest using?

- (A) Rule-Based Access Control (RAC)
- (B) Role-Based Access Control (RBAC)
- (C) Attribute-Based Access Control (ABAC)
- (D) Discretionary Access Control (DAC)

Question 418. You are an IT security professional for a large corporation. After receiving reports about some users being unable to access external websites, you decided to review the firewall logs. Which of the following would be a PRIMARY indicator in the logs that a rule is blocking outbound traffic?

- (A) Multiple entries of the same external IP address being ALLOWED
- (B) Timestamps showing large gaps between entries
- (C) Entries showing DROP/REJECT action for outbound traffic to port 80 and 443
- (D) Logs showing inbound traffic from multiple unknown external IP addresses

Question 419. DeltaCorp has a password policy in place which mandates users to change their passwords every 30 days.

However, some users complain that this results in them choosing simpler passwords or writing them down to remember them. How can DeltaCorp maintain security while addressing these concerns?

- (A) Reduce the password change frequency but introduce more complexity requirements

- (B) Eliminate password changes and rely solely on two-factor authentication
- (C) Ask users to change passwords every week to improve security
- (D) Allow users to reuse any of their last three passwords to ease the transition

Question 420. During a review of IDS logs, a security specialist notices a series of alerts indicating that a single external IP has been sending payloads that exploit a known vulnerability. However, the internal system to which these payloads are sent is patched and is not vulnerable to the exploit. Which of the following describes this type of IDS alert?

- (A) False positive
- (B) False negative
- (C) True positive
- (D) True negative

Question 421. A popular social media platform allows third-party applications to access user data and post on behalf of users. To avoid sharing user passwords with third-party applications and provide limited, scoped access, which authentication method should the platform use?

- (A) Embed user passwords in the application's code
- (B) Use basic authentication with username and password for every request
- (C) Implement Single Sign-On (SSO) using OAuth to provide token-based access
- (D) Rely solely on CAPTCHA for third-party app authentication

Question 422. An IT department in a large corporation spends several hours each day manually deploying patches and updates to thousands of workstations. Which of the following solutions would BEST enhance the efficiency of this process and save time for the IT team?

- (A) Disable automatic updates and conduct monthly patching sessions
- (B) Implement an automated patch management system
- (C) Designate a dedicated team for patching that operates in shifts
- (D) Educate users to install updates on their own

Question 423. An international company, GlobalTech, is using several web applications hosted by different vendors. To ensure their employees can access these applications without having to remember multiple sets of credentials, they want to implement a solution that can securely exchange user authentication information between the company and the service providers. What should GlobalTech implement?

- (A) Integrate each application with an independent LDAP server
- (B) Implement SSO using Security Assertions Markup Language (SAML)
- (C) Embed encrypted user credentials within the URL of each application
- (D) Rely on public API keys shared between the company and each vendor

Question 424. A company wants to implement a solution that verifies the software integrity of remote servers before allowing them to connect to the primary network. Which of the following

solutions BEST achieves this objective through attestation?

- (A) Host-based firewall
- (B) Whitelisting application
- (C) Remote attestation
- (D) VPN tunneling

Question 425. TechCorp is collaborating with SoftTech, a business partner. To streamline collaboration without managing multiple accounts, TechCorp wants its employees to use their existing credentials to access SoftTech's online project management system. Which of the following approaches would BEST enable this functionality?

- (A) TechCorp should create new accounts for its employees on SoftTech's system
- (B) SoftTech should allow anonymous access for TechCorp's employees
- (C) TechCorp should implement federation between its identity provider and SoftTech's service provider
- (D) SoftTech should reset all passwords and provide them to TechCorp's employees

Question 426. An organization recently experienced a malware infection on one of its workstations. A security analyst has been tasked with reviewing the endpoint logs of the infected system to gather more information about the incident. Which of the following entries in the endpoint logs would be MOST indicative of the initial malware infection point?

- (A) Logs indicating successful user login and logout events
- (B) Entries showing periodic system health-check status as "OK"
- (C) Logs documenting a recently installed and executed

unknown .exe file from a temporary directory

(D) Entries detailing network connectivity checks to the domain controller

Question 427. GammaTech has a new remote access policy for its employees. Whenever an employee attempts to access the corporate network from an unfamiliar location, the system requests additional verification before granting access. Which factor of authentication is being emphasized in this policy?

(A) Knowledge-based questions the employee answers

(B) A fingerprint scan from the employee

(C) The physical coordinates of the employee's access point

(D) An SMS code sent to the employee's phone

Question 428. AlphaTech's IT department is rolling out a new authentication protocol for remote workers. As part of the multifactor authentication process, employees are required to provide information that is memorized and cannot be physically taken from them. Which of the following represents this type of authentication factor?

(A) Fingerprint

(B) Smart card

(C) PIN

(D) USB security key

Question 429. A company has set up its firewall to allow web traffic through port 80 and port 443, while denying all other traffic by default. This setup is an example of which type of access control?

(A) Role-Based Access Control (RBAC)

(B) Mandatory Access Control (MAC)

- (C) Discretionary Access Control (DAC)
- (D) Rule-Based Access Control (RAC)

Question 430. The security team at WidgetCorp is trying to identify potential insider threats. They have set up a SIEM solution with a custom dashboard showing unusual activities. Which of the following dashboard views would be MOST effective for quickly identifying an employee uploading large amounts of proprietary data to an external cloud storage service?

- (A) Display of users who logged in during off-hours
- (B) Graph of highest network bandwidth users
- (C) List of most frequently used applications
- (D) Visualization of failed login attempts

Question 431. Sarah is a project manager and is working on a document that she owns. She wants to grant specific permissions to certain team members, allowing some to edit and others only to view the document. Which of the following access control models would BEST allow Sarah to accomplish this?

- (A) Mandatory Access Control (MAC)
- (B) Role-Based Access Control (RBAC)
- (C) Discretionary Access Control (DAC)
- (D) Attribute-Based Access Control (ABAC)

Question 432. CyberSec Corp's CISO wants to determine if there have been any anomalies in user behavior over the past month. Specifically, they're concerned about unauthorized data transfers outside of regular business hours. Which of the following automated reports would be MOST useful in this

investigation?

- (A) After-hours network activity reports
- (B) User password change frequency reports
- (C) Hardware inventory audit reports
- (D) Software licensing compliance reports

Question 433. After detecting suspicious activity on a network, a digital forensic analyst is dispatched to acquire data from a potential compromised system. The analyst decides to capture an image of the affected system's memory. This technique of capturing volatile data is particularly beneficial because:

- (A) It helps identify deleted files
- (B) It can capture data in real-time operations
- (C) It provides information on patch levels
- (D) It offers insights into firewall configurations

Question 434. During a suspected security incident involving unauthorized access to sensitive data, Jake, an IT administrator, immediately disconnected the affected server from the network. Later, a digital forensic expert criticized Jake's action. Which of the following is the MOST likely reason for the criticism?

- (A) Jake should have left the server connected to capture more evidence from the attacker
- (B) Jake should have immediately informed the company's legal department
- (C) Jake should have taken an image of the server's memory before disconnecting it
- (D) Jake should have updated the server's software to prevent further unauthorized access

Question 435. A large enterprise is deploying a new automation system that will allow various teams, including development, operations, and QA, to provision and configure their own environments. The security team is concerned about potential misconfigurations or excessive permissions being granted. Which solution can be used within the automation to ensure security standards are met without limiting the agility of the teams?

- (A) Implementing a zero-trust model for all teams
- (B) Manually reviewing all requests before provisioning
- (C) Setting up guard rails within the automation scripts to define boundaries and prevent misconfigurations
- (D) Disabling the automation system for all teams except the security team

Question 436. After a security breach, Jake, a digital forensics investigator, arrives at the scene to collect a hard drive for examination. He labels the hard drive, records its serial number, photographs the scene, and ensures the hard drive is transported securely to the forensics lab. These steps are crucial to:

- (A) Preserve the data's integrity on the hard drive
- (B) Maintain the chain of custody
- (C) Decrypt the data on the hard drive
- (D) Implement a legal hold on the data

Question 437. After deploying a new version of your company's internal application, several users reported issues with accessing specific features. To investigate the root cause, you decided to review the application logs. What entry in the logs would most directly indicate a software bug or error related to the recent deployment?

- (A) Entries showing successful user authentication timestamps
- (B) Entries detailing the number of transactions completed by the application
- (C) Entries with "ERROR" or "EXCEPTION" related to the specific feature being accessed
- (D) Entries showing routine data backup operations

Question 438. After a major data breach in XYZ Corporation, the management decided to understand the primary reason behind the incident to prevent such occurrences in the future. Which of the following approaches should the incident response team prioritize to determine the fundamental cause of the breach?

- (A) Perform vulnerability scanning on all servers
- (B) Review firewall logs for the past week
- (C) Conduct a root cause analysis
- (D) Upgrade all security software

Question 439. A cloud infrastructure team frequently receives performance alerts from various resources in the environment. They want to ensure that relevant teams are immediately informed and can act upon any resource that crosses a performance threshold. What is the BEST way to accomplish this?

- (A) Conduct a weekly meeting to review all performance alerts
- (B) Automate ticket creation for any resource that crosses the performance threshold and assign it to the relevant team
- (C) Send all performance alerts to the cloud infrastructure

team's email for review

(D) Disable performance monitoring to reduce alert fatigue

Question 440. A development team is working on a mission-critical application for a financial institution. The team wants to ensure that any code changes do not introduce vulnerabilities or break existing functionalities. What is the BEST automation approach to achieve this objective?

(A) Manually review the code changes once a month

(B) Use continuous integration tools to automatically compile and test code changes against known vulnerabilities and functional tests

(C) Rely on users to report any issues after the application is deployed

(D) Implement a firewall to block potential attacks on the application

Question 441. Acme Corp. is in the early stages of a potential lawsuit, and their legal department has just issued a notice for e-discovery related to email communications of a former executive. As an IT security professional, which of the following should be your FIRST action?

(A) Start a full backup of the company's email server

(B) Identify and isolate the email accounts related to the former executive

(C) Immediately delete all emails that are more than two years old

(D) Inform the media about the upcoming lawsuit

Question 442. OmegaHealth, a large healthcare provider, is integrating automation into its operations. When a new

healthcare worker is hired, they require access to multiple systems. Why would OmegaHealth automate the user provisioning process across these systems?

- (A) To enforce a uniform password for all healthcare workers.
- (B) To save time by ensuring consistent and simultaneous account creation across all necessary platforms
- (C) To prevent the new hires from accessing any system until their probation period ends
- (D) To reduce the software licenses needed by delaying account activation

Question 443. During a regular review of system logs, Alex, a security analyst, noticed an unusual pattern of network traffic originating from a single IP address. Instead of waiting for an automated system to flag this as suspicious, he decides to manually dive deeper into the data to identify any potential threats. What is Alex engaging in?

- (A) Incident management
- (B) Threat modeling
- (C) Threat hunting
- (D) Security monitoring

Question 444 OmegaTech's security team noticed an increase in account compromises. An internal investigation revealed that many employees have been using the same passwords across different company systems and applications. Which password best practice can OmegaTech enforce to mitigate this issue?

- (A) Encouraging users to change their passwords every month
- (B) Implementing an account lockout policy after three

failed login attempts

(C) Prohibiting password reuse for at least the last five password changes

(D) Mandating that passwords contain only alphabetical characters for simplicity

Question 445. AlphaCorp's IT department is reviewing password policies and wants to adopt a strategy that enhances security. Which of the following password strategies would be the MOST secure?

(A) Passwords should be at least 6 characters long, with no other requirements

(B) Passwords should be at least 10 characters long and include both uppercase and lowercase letters

(C) Passwords should be at least 8 characters long and include uppercase letters, lowercase letters, numbers, and special characters

(D) Passwords should be at least 4 characters long and include a mix of uppercase and lowercase letters

Question 446. A security analyst is reviewing the IPS logs and discovers multiple alerts originating from a single IP address attempting to access various company servers. The analyst is trying to determine the type of attack. Which of the following log entries BEST indicates a port scanning activity?

(A) Multiple consecutive connection attempts to different ports on a single server in a short time frame

(B) Repeated connection attempts to port 80 of a web server every 3 seconds

(C) Numerous failed login attempts to an FTP server from the same IP address

(D) Consistent pings to the network gateway every 5 seconds

Question 447. As part of a cloud infrastructure project, AlphaTech plans to deploy multiple virtualized resources for its new application. The deployment includes databases, web servers, and load balancers. What is the PRIMARY benefit of using automation scripts in the resource provisioning process for this project?

- (A) It enables AlphaTech to use a single operating system for all resources
- (B) It guarantees 100% uptime for all virtualized resources
- (C) It ensures standardized, repeatable, and rapid deployments across the infrastructure
- (D) It prevents unauthorized users from accessing the cloud infrastructure

Question 448. DeltaTech, a progressive tech firm, is aiming to improve its security posture by eliminating the vulnerabilities associated with password use. They are considering deploying a passwordless authentication system. Which of the following represents the PRIMARY advantage of such a system?

- (A) It allows users to choose any password complexity
- (B) It eliminates the need for remembering passwords
- (C) It guarantees protection against all cyber threats
- (D) It ensures compatibility with all legacy systems

Question 449. OmegaTech recently introduced an additional layer of security for its remote server access. Along with their usual passwords, employees now need to use a physical device they have with them to gain access. Which of the following

represents this “something you have” factor in multifactor authentication?

- (A) Password hint
- (B) Facial recognition
- (C) Hardware token
- (D) Voice recognition

Question 450. A large corporation is investigating a potential insider threat incident. A security analyst is tasked with examining the OS-specific security logs of a Windows server where sensitive documents are stored. Which of the following entries in the logs would MOST likely indicate unauthorized access attempts?

- (A) Logs displaying Windows Update successful installations
- (B) Entries showing a large number of failed login attempts followed by a successful login from a user outside of regular business hours
- (C) Logs indicating scheduled disk defragmentation tasks
- (D) Entries detailing successful printer connections and print jobs

Question 451. ThetaTech, a financial institution, wants to upgrade its authentication system for high-net-worth customers accessing their accounts online. Besides the traditional password, they want to include a method that captures unique physical or behavioral characteristics. Which type of authentication method should ThetaTech consider?

- (A) Token-based authentication
- (B) Geolocation tracking

- (C) Biometrics
- (D) Smart card

Question 452. The cybersecurity team of XYZ Corp. plans to assess their organization's preparedness for a potential data breach. They aim to evaluate the effectiveness of their response strategy without performing any real actions. Which of the following methods would BEST help them achieve this goal?

- (A) Live fire exercise
- (B) System hardening test
- (C) Red team/blue team exercise
- (D) Tabletop exercise

Question 453. In preparation for a potential lawsuit, Meg, a cybersecurity analyst, has been asked to ensure that specific digital evidence remains intact and is not altered or deleted. What measure should Meg implement to ensure this requirement?

- (A) Encrypt the evidence
- (B) Initiate a legal hold
- (C) Perform a full disk wipe
- (D) Conduct a vulnerability assessment

Question 454. A financial company is designing a new system that needs to ensure data is accessed based on classifications and clearance levels of the users. Which of the following access control models BEST fits this requirement?

- (A) Role-Based Access Control (RBAC)
- (B) Discretionary Access Control (DAC)
- (C) Mandatory Access Control (MAC)
- (D) Attribute-Based Access Control (ABAC)

Question 455. The incident response team at XYZ Corp received a report that an attacker successfully exploited a vulnerable web application in their environment. To identify which server might have been compromised, the team decided to cross-reference recent vulnerability scan results. Which of the following information from the vulnerability scan would be MOST helpful in pinpointing the potentially compromised server?

- (A) The timestamp of when the scan was conducted
- (B) The software version of the scanning tool
- (C) List of hosts with the specific vulnerability related to the exploit
- (D) The total number of vulnerabilities identified during the scan

Question 456. Epsilon Inc. recently hired Jenny as a junior network administrator. To ensure security, they give Jenny only the access permissions necessary to complete her specific tasks, such as monitoring network traffic, but not modifying firewall rules. This approach of granting Jenny's permissions aligns with which security principle?

- (A) Mandatory Access Control (MAC)
- (B) Role-Based Access Control (RBAC)
- (C) Time-of-Day Restrictions
- (D) Least Privilege

Question 457. A company is attempting to verify the legitimacy of an email sent from a senior executive to a number of employees. The email requests the recipients to click on a link and enter their credentials for a "system upgrade." The security team wants to ascertain if the email genuinely came from the

executive. Which of the following metadata from the email would be MOST beneficial in this investigation?

- (A) The email's subject line
- (B) The email's send time and date
- (C) The originating IP address in the email headers
- (D) The size of the email in bytes

Question 458. A cloud-based e-commerce company wants to ensure that its inventory system automatically updates the stock levels on its website and third-party sales platforms whenever a sale occurs. What should the company leverage to achieve this real-time synchronization?

- (A) Regularly backup the inventory system and restore it on the website and sales platforms
- (B) Rely on customers to report discrepancies in stock levels
- (C) Use Application Programming Interfaces (APIs) to integrate the inventory system with the website and third-party platforms
- (D) Conduct daily stock audits and manually update all platforms

Question 459. After a series of phishing attacks, the IT department of BetaTech Corp noticed that several employees were using easily guessable passwords. The security team decided to recommend the use of password managers to assist employees in creating and remembering strong passwords. Which of the following is a PRIMARY benefit of using password managers in this context?

- (A) Password managers automatically update the operating system
- (B) Password managers can generate and store complex

passwords

- (C) Password managers always prevent phishing attacks
- (D) Password managers allow the reuse of strong passwords across multiple platforms

Question 460. A company's online retail website faces DDoS attacks that cause significant downtime. Their current setup relies on manual verification of traffic spikes before mitigation efforts are deployed. What change could BEST enhance the company's reaction time to such attacks in the future?

- (A) Educate users to report slow website loading times
- (B) Manually back up the website data every hour
- (C) Deploy a web application firewall with automated DDoS mitigation features
- (D) Increase the website's bandwidth to handle traffic spikes

Answers 311-460

Question 311. A financial institution is shutting down one of its data centers. Given the highly sensitive nature of the data stored, the company wants to ensure that there is no possibility of data retrieval from the storage devices. Which of the following methods would be the MOST effective in guaranteeing the destruction of data?

- (A) Overwriting with zeros
- (B) Standard Disk Format

- (C) **Physical Destruction**
- (D) Running a Disk Cleanup utility

Explanation 311. Correct Answer: C. Physical Destruction.

Physical destruction, such as shredding or incinerating the storage devices, ensures complete destruction of the media, making data retrieval impossible, regardless of the tools or techniques employed.

Option A is incorrect. Overwriting with zeros is a method of data sanitization, but advanced techniques might still retrieve some portions of the data.

Option B is incorrect. A standard disk format often does not remove data entirely, and traces can remain that could be recovered with specialized software.

Option D is incorrect. Disk Cleanup utilities are designed to free up space by removing temporary and unnecessary files but not to securely erase sensitive data.

Question 312. A financial application allows users to transfer money to other accounts by entering the account number and the amount to transfer. During a security audit, it was observed that malicious users could enter SQL code into the account number field to manipulate the application's database. Which security technique should the development team implement to address this vulnerability?

- (A) Code obfuscation
- (B) **Input validation**

- (C) Encryption at rest
- (D) Session timeout

Explanation 312. Correct Answer: B. Input validation. Input validation ensures that only valid and expected data is accepted by an application. By validating and sanitizing user input, the application can prevent malicious data, such as SQL code, from being processed and executed, thus mitigating the risk of SQL injection attacks.

Option A is incorrect. Code obfuscation makes it more difficult for attackers to understand the application's code but does not prevent them from injecting malicious input.

Option C is incorrect. Encryption at rest protects stored data, but it doesn't prevent SQL injection attacks which exploit the application's input handling.

Option D is incorrect. Session timeout limits the duration of a user's session, but it does not validate or sanitize user input.

Question 313. After a series of cyberattacks, BetaTech, a financial institution, decided to standardize the configurations across its entire server fleet. They've established a secure baseline configuration for their servers. What should be the NEXT step in ensuring the servers conform to this new baseline?

- (A) Frequently conduct vulnerability scanning on all servers
- (B) Introduce biometric authentication for server access
- (C) **Deploy the secure baseline across all servers**
- (D) Monitor network traffic to detect anomalies

Explanation 313. Correct Answer: C. Deploy the secure baseline across all servers. After establishing a secure baseline, the immediate next step is to deploy or apply this baseline to the servers. This ensures that all servers start from a standardized and secure configuration.

Option A is incorrect. While vulnerability scanning is crucial, it is more of a continuous process to identify potential vulnerabilities and doesn't directly apply the secure baseline to the servers.

Option B is incorrect. Biometric authentication, though a valuable security measure, does not address the deployment of the established secure baseline on servers.

Option D is incorrect. Monitoring network traffic is essential for detecting potential threats, but it does not directly ensure the deployment of the secure baseline on servers.

Question 314. An energy company is looking to enhance the security of its ICS/SCADA systems. They have realized that default configurations might have vulnerabilities. Which of the following is the BEST initial step to take in securing their ICS/SCADA systems?

- (A) Connect the ICS/SCADA systems to the internet for remote monitoring
- (B) Use commercial off-the-shelf software to add a layer of security
- (C) **Implement a secure baseline configuration tailored to the ICS/SCADA environment**

(D) Increase the number of users with administrative privileges to ensure rapid response to issues

Explanation 314. Correct Answer: C. Implement a secure baseline configuration tailored to the ICS/SCADA environment.

Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems are critical in managing industrial processes. Implementing a secure baseline configuration tailored to these systems ensures that unnecessary services and potential vulnerabilities are minimized.

Option A is incorrect. Connecting ICS/SCADA systems directly to the internet exposes them to a wide range of threats and potential cyber-attacks.

Option B is incorrect. While commercial off-the-shelf software can be beneficial, it's not the best initial step. Secure baselines tailored to the ICS/SCADA environment are more effective.

Option D is incorrect. Increasing the number of users with administrative privileges contradicts the principle of least privilege and can introduce more security vulnerabilities.

Question 315. A multinational company is planning to issue company-owned mobile devices to its executives. Given the sensitivity of the data the executives handle, what hardening measure would be MOST effective to ensure the security of these mobile devices?

(A) Regularly updating the company's social media profiles to mention the security measures taken

- (B) **Implementing biometric authentication in addition to strong passcodes**
- (C) Turning off Bluetooth and Wi-Fi when not in use
- (D) Setting the devices to display brighter screen colors

Explanation 315. Correct Answer: B. Implementing biometric authentication in addition to strong passcodes.

Biometric authentication (like fingerprint or facial recognition) combined with strong passcodes provides a robust multi-factor authentication mechanism, making unauthorized access to the device significantly more challenging.

Option A is incorrect. Publicly announcing security measures on social media does not harden the device. Moreover, divulging too much about security practices could expose the organization to targeted attacks.

Option C is incorrect. While turning off Bluetooth and Wi-Fi can reduce certain attack vectors, it's not as comprehensive a security measure as implementing strong multi-factor authentication.

Option D is incorrect. Screen colors have no direct correlation to the security hardening of a device.

Question 316. A large e-commerce company wants to ensure that their newly developed application is free from any code vulnerabilities before it is deployed to the production environment. They want to catch any software flaws, especially those that might lead to potential security risks. Which of the following methodologies should they employ?

- (A) Runtime application self-protection (RASP)
- (B) Penetration testing on the live application
- (C) **Static code analysis**
- (D) User acceptance testing (UAT)

Explanation 316. Correct Answer: C. Static code analysis.

Static code analysis involves analyzing the application's code without executing it, focusing on detecting vulnerabilities, coding flaws, or other potential security threats, making it an appropriate methodology for the scenario presented.

Option A is incorrect. Runtime application self-protection (RASP) is about real-time application monitoring and protection, which would not be the primary choice for pre-deployment vulnerability checks.

Option B is incorrect. Penetration testing on the live application involves testing the application once it is live or running, which might not be suitable when looking to identify vulnerabilities in the pre-deployment phase.

Option D is incorrect. User acceptance testing (UAT) focuses on determining if the software meets the business needs and functions correctly for the end-users. It does not emphasize finding security vulnerabilities.

Question 317. Jenny, the new CIO of a multinational firm, wants to ensure that every software and hardware asset in the organization has a clearly defined owner responsible for its security and maintenance. Which of the following is the MOST effective way to achieve this?

- (A) Deploy an automated asset discovery tool and assign assets to departments based on their location
- (B) Mandate that every department head is the default owner of all assets within their department
- (C) Conduct regular audits and require individual users to claim ownership of their assets
- (D) Introduce an Asset Management System where assets are logged with defined ownership as they are procured or assigned**

Explanation 317. Correct Answer: D. Introduce an Asset Management System where assets are logged with defined ownership as they are procured or assigned. An Asset Management System provides a structured way to log, track, and manage assets throughout their lifecycle, including defining and recording asset ownership. This ensures clarity and accountability regarding asset responsibility.

Option A is incorrect. While automated discovery tools are helpful, assigning assets based solely on location does not necessarily reflect the actual usage or responsibility for the asset.

Option B is incorrect. While department heads should be aware of assets within their departments, they may not always be the best individuals to take ownership, especially for specific or specialized assets.

Option C is incorrect. Regular audits are crucial, but relying solely on users to claim ownership might not capture all assets, and it's a reactive rather than proactive approach.

Question 318. An audit report indicates that several network switches in a data center lack security configurations, making them potential targets for attackers. Which of the following hardening techniques would BEST reduce the risk associated with these switches?

- (A) Configuring port mirroring to monitor network traffic
- (B) **Disabling unused switch ports**
- (C) Implementing load balancing across the switches
- (D) Increasing the MAC address table size for performance

Explanation 318. Correct Answer: B. Disabling unused switch ports. By disabling unused switch ports, you minimize potential points of entry for unauthorized devices or attackers. This is a basic step in network switch hardening.

Option A is incorrect. Port mirroring is used for monitoring and isn't directly a hardening technique. While monitoring is crucial for security, it doesn't necessarily prevent unauthorized access.

Option C is incorrect. Load balancing is primarily about distributing network traffic efficiently across multiple paths or resources, and it doesn't inherently harden the switches.

Option D is incorrect. Increasing the MAC address table size might improve switch performance in certain scenarios, but it does not harden the switch against potential security threats.

Question 319. DeltaSoft has released a new web application. The security team is tasked with observing the application's behavior and responses when it is running to identify potential

vulnerabilities. Which method is most appropriate for this purpose?

- (A) Static Analysis
- (B) Fuzz Testing
- (C) Whitebox Testing
- (D) **Dynamic Analysis**

Explanation 319. Correct Answer: D. Dynamic Analysis.

Dynamic analysis focuses on examining an application during its execution, or runtime. By observing the application's behavior and responses, security teams can identify vulnerabilities that might not be evident in the static code.

Option A is incorrect. Static analysis evaluates an application's code without executing the application. It does not focus on observing the application's behavior during runtime.

Option B is incorrect. Fuzz testing involves submitting random inputs to an application to observe its behavior and detect vulnerabilities, but it's just one subset of dynamic analysis.

Option C is incorrect. Whitebox testing involves understanding the internal structures and workings of an application while testing, which can be part of static or dynamic testing, but on its own, it does not specifically focus on runtime behavior observation.

Question 320. A security analyst at ZetaTech is looking to gather information about emerging threats and vulnerabilities relevant to their industry. Which of the following would be the MOST suitable method to obtain real-time, continuously

updated data on potential security issues?

- (A) Relying solely on automated internal vulnerability scanners
- (B) Periodic manual penetration testing
- (C) **Subscribing to an OSINT threat feed**
- (D) Regularly checking the company's firewall logs

Explanation 320. Correct Answer: C. Subscribing to an OSINT threat feed. An OSINT (Open-source intelligence) threat feed provides real-time information and is continuously updated with data on potential security issues sourced from publicly available information.

Option A is incorrect. While automated internal vulnerability scanners are valuable for identifying vulnerabilities within the organization's infrastructure, they don't provide continuous real-time data about external emerging threats.

Option B is incorrect. Manual penetration testing is periodic and doesn't offer continuous updates on emerging threats from the broader industry.

Option C is incorrect. Regularly checking the company's firewall logs will give insight into potential malicious activities targeting the company, but it won't offer broad, updated data on industry-wide threats.

Question 321. A medium-sized enterprise is preparing to upgrade its office workstations. The IT department is considering purchasing devices from a lesser-known, but cheaper, vendor. Which of the following should be the

PRIMARY consideration before finalizing the acquisition?

- (A) Whether the vendor offers a longer warranty period
- (B) The aesthetics and design of the workstations
- (C) **The vendor's adherence to industry security standards and practices**
- (D) The amount of training required for IT staff to support the new devices

Explanation 321. Correct Answer: C. The vendor's adherence to industry security standards and practices.

Ensuring that the vendor adheres to industry security standards and practices is critical for maintaining a secure environment. Devices that don't meet security standards could introduce vulnerabilities into the organization.

Option A is incorrect. While a longer warranty period might be attractive, it should not be the primary concern over security considerations.

Option B is incorrect. Aesthetics and design, while potentially important for branding or user satisfaction, are not as critical as security considerations.

Option D is incorrect. Training the IT staff is important, but it shouldn't take precedence over ensuring the devices themselves are secure.

Question 322. ClearView Industries wants to give their employees the flexibility to choose their own devices for work while retaining control over the device configurations and applications. Which deployment model would be the MOST

appropriate for ClearView's objectives?

- (A) Bring Your Own Device (BYOD)
- (B) **Choose Your Own Device (CYOD)**
- (C) Corporate-owned, Personally Enabled (COPE)
- (D) Fixed Device Deployment (FDD)

Explanation 322. Correct Answer: B. Choose Your Own Device (CYOD). In the CYOD model, employees are allowed to choose a device from a list of approved devices. The organization retains control over the device configurations and applications, ensuring a blend of user preference and corporate security.

Option A is incorrect. BYOD allows employees to bring their personal devices to work, which means the organization has less control over the configurations and applications.

Option C is incorrect. While COPE provides devices owned by the corporation and allows personal use, it does not necessarily offer employees the choice of which device they get.

Option D is incorrect. Fixed Device Deployment (FDD) is not a standard deployment model in the context of mobile solutions, and it does not reflect the flexibility of device choice.

Question 323. A recently hired security analyst at CyberTech Inc. wants to get a better understanding of the organization's network infrastructure. Which of the following activities would provide a LIST of servers, workstations, printers, switches, and routers currently active in the network?

- (A) Vulnerability Scanning

- (B) Intrusion Detection
- (C) **Network Enumeration**
- (D) Penetration Testing

Explanation 323. Correct Answer: C. Network

Enumeration. Network enumeration is the process of identifying devices on a network. Through enumeration, an analyst can gather information about network devices, their types, and other attributes, thereby getting a clearer picture of the network's infrastructure.

Option A is incorrect. Vulnerability scanning aims to identify vulnerabilities in network devices and systems, not necessarily to list all active devices.

Option B is incorrect. Intrusion detection focuses on monitoring network traffic for malicious activities and potential security breaches.

Option D is incorrect. Penetration testing aims to exploit vulnerabilities in a network to determine its security posture, not to list all active devices.

Question 324. A network engineer is preparing a new batch of routers for deployment in a large organization. Which of the following steps should the engineer prioritize to ensure that the routers are securely configured from the start?

- (A) Configure the routers to use DHCP to dynamically assign IP addresses to connected devices
- (B) **Change the default administrative credentials on the routers**

- (C) Update the routers' firmware to the latest, most feature-rich version, regardless of its security posture
- (D) Customize the routers' LED colors for easy identification in the server room

Explanation 324. Correct Answer: B. Change the default administrative credentials on the routers. Routers often come with default credentials that are widely known and can be easily exploited by attackers. Changing these credentials is essential for establishing a secure baseline.

Option A is incorrect. While DHCP is commonly used in many networks, enabling it is not necessarily a secure baseline action. Additionally, DHCP on routers can be exploited if not securely configured.

Option C is incorrect. Blindly updating to the latest firmware without considering its security posture can introduce vulnerabilities. It's important to ensure that the firmware is both updated and secure.

Option D is incorrect. Customizing LED colors relates to physical identification and does not inherently improve the security configuration of a router.

Question 325. A university is looking to revamp its wireless network to provide secure access for students and faculty. The IT department wants an authentication method that leverages a centralized server to validate user credentials and can integrate with their existing directory service. Which authentication protocol should they consider?

- (A) Pre-shared Key (PSK)
- (B) Lightweight Extensible Authentication Protocol (LEAP)
- (C) **Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)**
- (D) Shared Secret Challenge

Explanation 325. Correct Answer: C. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). EAP-TLS provides strong security by using digital certificates to authenticate both the client and the server. It operates in conjunction with a RADIUS server, allowing for centralized management of user credentials and seamless integration with existing directory services.

Option A is incorrect. Pre-shared Key (PSK) does not involve a centralized server for authentication. Instead, a single shared key is used for all devices, which may not be scalable or secure for a large university setting.

Option B is incorrect. While LEAP provides centralized authentication via a RADIUS server, it has known vulnerabilities and may not offer the level of security the university is looking for.

Option D is incorrect. Shared Secret Challenge is not a standard wireless authentication protocol. In practice, challenges based on shared secrets (like PSK) can be vulnerable if the secret becomes known.

Question 326. TechHive Corp. is planning to sell some of its old servers. Before selling, they want to ensure that no

retrievable personal or business data remains on the hard drives. Which of the following methods should TechHive use to ensure the drives are clean and the data cannot be recovered?

- (A) Simple Format
- (B) **Magnetic Wiping**
- (C) Physical Destruction
- (D) Standard Defragmentation

Explanation 326. Correct Answer: B. Magnetic Wiping.

Magnetic wiping, also known as degaussing, uses magnetic fields to permanently erase data from storage devices. It makes the data irretrievable, ensuring that personal and business data cannot be recovered even with advanced tools.

Option A is incorrect. A simple format often leaves traces of data, which can potentially be recovered using specialized software.

Option C is incorrect. While physical destruction ensures data cannot be retrieved, it would make the servers unusable for resale purposes.

Option D is incorrect. Defragmentation is a process to optimize and organize the data on a drive, but it does not erase data.

Question 327. The network administrator of a rapidly growing tech firm is concerned about the potential vulnerabilities of the company's switches. Which of the following measures is MOST effective in hardening these network switches against possible attacks?

- (A) Assigning static IP addresses to all connected devices
- (B) **Implementing strong password policies for switch access**
- (C) Upgrading the switches to support 10Gbps for future expansion
- (D) Customizing the switch LED colors for easy identification

Explanation 327. Correct Answer: B. Implementing strong password policies for switch access. Hardening switches involves reducing their vulnerability to unauthorized access and potential misuse. Implementing strong password policies ensures that only authorized personnel can access and configure the switches.

Option A is incorrect. While assigning static IP addresses might help in network management, it does not inherently harden a switch against potential attacks.

Option C is incorrect. Upgrading the speed capabilities of switches, such as supporting 10Gbps, is a performance enhancement and not directly related to hardening or security.

Option D is incorrect. Customizing LED colors is related to physical identification and does not improve the security posture of the switch.

Question 328. A robotics company is developing an autonomous vehicle that relies on a Real-Time Operating System (RTOS) to manage its operations. The development team wants to ensure that the vehicle's RTOS has a solid

security posture. What should the team prioritize when establishing a secure baseline for this RTOS?

- (A) Installing a robust antivirus software
- (B) Enabling all features for maximum functionality
- (C) Regularly backing up the RTOS data to the cloud
- (D) **Minimizing the number of services and open ports**

Explanation 328. Correct Answer: D. Minimizing the number of services and open ports. Reducing the number of services and open ports reduces the attack surface on the RTOS, making it more challenging for attackers to find vulnerabilities.

Option A is incorrect. While antivirus software is essential for many systems, an RTOS, especially one for an autonomous vehicle, would prioritize reducing the attack surface and ensuring real-time performance rather than relying on traditional antivirus solutions.

Option B is incorrect. Enabling all features may introduce unnecessary vulnerabilities. It's best to enable only required functionalities to maintain security.

Option C is incorrect. While backups are crucial for data integrity and recovery, the primary concern for an RTOS, especially in autonomous vehicles, would be real-time performance and reducing potential vulnerabilities.

Question 329. After deploying wireless access points in a large manufacturing facility, employees report inconsistent wireless connectivity in some areas. What tool would be most effective for the IT team to use to visualize areas of weak wireless signal

strength?

- (A) Network bandwidth monitor
- (B) Protocol analyzer
- (C) **Heat map software**
- (D) Intrusion detection system

Explanation 329. Correct Answer: C. Heat map software.

Heat map software allows IT professionals to visually see areas of strong and weak wireless signal strength, making it easier to adjust placements or add additional access points as needed.

Option A is incorrect. A network bandwidth monitor is used to measure the amount of data being sent over a network, not to visualize wireless signal strength.

Option B is incorrect. A protocol analyzer is used to capture and analyze network traffic, not to visually display wireless coverage.

Option D is incorrect. An intrusion detection system (IDS) is designed to detect unauthorized access or malicious activities on a network. It does not show areas of weak wireless signal strength.

Question 330. Sarah, an end-user, downloads a software update from a website. Before installing, she wants to make sure the software hasn't been modified maliciously and that it originates from a trusted source. What should Sarah check to validate this?

- (A) The SSL certificate of the website
- (B) **The application's code signing certificate**

- (C) The application's open-source repositories
- (D) The software's user reviews

Explanation 330. Correct Answer: B. The application's code signing certificate. By checking the application's code signing certificate, Sarah can validate that the software was indeed issued by a trusted entity and hasn't been altered since it was signed. A valid code signing certificate gives users confidence in the authenticity and integrity of the software.

Option A is incorrect. While the SSL certificate of a website ensures secure data transmission between the server and the browser, it doesn't guarantee the integrity or authenticity of the software being downloaded.

Option C is incorrect. Open-source repositories may contain the source code of a software, but checking these repositories doesn't necessarily validate the integrity of the compiled software version Sarah has downloaded.

Option D is incorrect. User reviews can provide insights into the software's functionality and user experience, but they cannot be relied upon to confirm software authenticity or integrity.

Question 331. A local coffee shop offers free Wi-Fi to its customers. Recently, there have been reports of man-in-the-middle attacks on the network. The owner decides to upgrade the wireless security and wants to implement a cryptographic protocol to secure data transmissions. Which protocol would provide a balance between security and performance for the public Wi-Fi users?

- (A) **Advanced Encryption Standard (AES)**
- (B) Wired Equivalent Privacy (WEP)
- (C) RC4 Stream Cipher
- (D) Open Wireless

Explanation 331. Correct Answer: A. Advanced Encryption Standard (AES). AES offers a good balance between security and performance. It is a modern encryption standard that provides strong security without causing significant performance overhead, making it suitable for a public Wi-Fi setting where both security and user experience are important.

Option B is incorrect. WEP is an outdated encryption protocol with known vulnerabilities. It is insecure and can be easily cracked, making it unsuitable for securing a public Wi-Fi network.

Option C is incorrect. RC4 is a stream cipher that was used in older wireless protocols like WEP. It has been found to be vulnerable to various attacks and is no longer considered secure for wireless networks.

Option D is incorrect. An open wireless network does not implement any encryption, leaving data transmissions vulnerable to eavesdropping and other attacks. It would not provide the desired security for the coffee shop's Wi-Fi users.

Question 332. A software development company has decided to host their applications in a multi-cloud environment. Before deploying, they are looking to enhance the security of their cloud-based resources. Which of the following is the BEST

practice for hardening their cloud infrastructure?

(A) Ensure that all cloud storage buckets or containers are publicly accessible for easier data sharing

(B) **Apply consistent security configurations and policies across all cloud providers**

(C) Use the same SSH key pairs across all cloud instances for uniformity

(D) Limit the use of Identity and Access Management (IAM) roles to senior staff only

Explanation 332. Correct Answer: B. Apply consistent security configurations and policies across all cloud providers.

Maintaining consistent security configurations and policies across all cloud providers ensures that there are no weak links in the multi-cloud setup and reduces the complexity of managing multiple sets of policies.

Option A is incorrect. Making all cloud storage buckets or containers publicly accessible can expose sensitive data and is a common misconfiguration that leads to data breaches.

Option C is incorrect. Using the same SSH key pairs across all instances can be risky. If an attacker obtains the SSH key, they can gain unauthorized access to all instances that use that key.

Option D is incorrect. While it's important to limit access based on the principle of least privilege, IAM roles should be appropriately assigned to staff based on their responsibilities and not just their seniority. This ensures that users have the necessary permissions to do their jobs without unnecessary access to sensitive resources.

Question 333. After running a vulnerability scan on the company's infrastructure, a security analyst notices a reported vulnerability on a server. However, after manual verification, the analyst determines that the vulnerability doesn't actually exist on the server. What is this situation best described as?

- (A) A false negative
- (B) A true positive
- (C) **A false positive**
- (D) A confirmation bias

Explanation 333. Correct Answer: C. A false positive. A false positive in vulnerability management occurs when a system incorrectly flags a threat or vulnerability that isn't truly present. This can lead to wasted resources on investigating and attempting to remediate a non-existent issue.

Option A is incorrect. A false negative would mean that the vulnerability exists, but the system failed to detect it, which is the opposite of the scenario described.

Option B is incorrect. A true positive means that the vulnerability was correctly identified and truly exists, which isn't the case here.

Option D is incorrect. Confirmation bias is a cognitive bias where one favors information that confirms their existing beliefs. It's not relevant to the scenario of incorrectly detected vulnerabilities.

Question 334. An e-commerce platform recently suffered a data breach where attackers exploited cookies to impersonate user

sessions. A security analyst is tasked with recommending measures to secure user cookies. Which of the following measures will ensure that cookies are transmitted securely between the user's browser and the server?

- (A) Storing cookies in the database
- (B) **Implementing the "Secure" attribute for cookies**
- (C) Increasing the cookie expiration time
- (D) Base64 encoding the cookie content

Explanation 334. Correct Answer: B. Implementing the "Secure" attribute for cookies. The "Secure" attribute ensures that a cookie is only sent over secure, encrypted HTTPS connections. By implementing this attribute, the cookie won't be transmitted over unencrypted HTTP connections, reducing the risk of interception by malicious actors.

Option A is incorrect. Storing cookies in the database doesn't necessarily secure the transmission of cookies between the client and server. It's more about storage security rather than transmission security.

Option C is incorrect. Increasing the cookie expiration time can actually increase the window of opportunity for an attacker to exploit a cookie, making it a less secure practice.

Option D is incorrect. Base64 encoding is not encryption; it's just a way to represent binary data in an ASCII string format. Encoding can be easily reversed, offering little to no security.

Question 335. A security analyst is reviewing a vulnerability report and sees a reference to CVE-2023-12345 with a CVSS

score of 9.5. Which of the following conclusions can the analyst draw based on this information?

- (A) **The vulnerability was first identified in the year 2023**
- (B) The vulnerability is of low severity
- (C) The vulnerability affects only software produced in 2023
- (D) CVE-2023-12345 is the software vendor's internal code for the vulnerability

Explanation 335. Correct Answer: A. The vulnerability was first identified in the year 2023. The CVE identifier's format begins with the year the vulnerability was made public, so CVE-2023-12345 indicates a vulnerability identified in 2023.

Option B is incorrect. CVSS scores range from 0 to 10, with higher scores indicating higher severity. A score of 9.5 is considered critical severity, not low.

Option C is incorrect. The year in a CVE identifier refers to when the vulnerability was published, not the year the software was produced.

Option D is incorrect. The CVE system is a standard method for identifying vulnerabilities and doesn't represent a software vendor's internal coding.

Question 336. AlphaTech is seeking a comprehensive source of intelligence about the latest cyber threats targeting its specific industry. While OSINT provides valuable data, the company is considering investing in a more specialized solution. Which of the following would best address AlphaTech's needs?

- (A) Implementing internal honeypots to trap attackers
- (B) **Subscribing to a third-party threat intelligence feed**
- (C) Regularly attending cyber security conferences
- (D) Using open-source vulnerability scanners

Explanation 336. Correct Answer: B. Subscribing to a third-party threat intelligence feed. A third-party threat intelligence feed, especially one tailored for a specific industry, provides specialized, often real-time information about cyber threats, offering insights beyond what's available in the public domain.

Option A is incorrect. While honeypots can help understand the tactics of attackers targeting the organization, they don't provide comprehensive intelligence about industry-wide threats.

Option C is incorrect. Attending cyber security conferences can offer insights and updates, but it's not a continuous or real-time source of threat intelligence.

Option D is incorrect. Open-source vulnerability scanners help identify vulnerabilities within an organization's infrastructure but don't offer specialized intelligence about industry-specific cyber threats.

Question 337. ABC Corp recently adopted a Bring Your Own Device (BYOD) policy. The IT department is concerned about the potential risks associated with personal devices accessing the corporate network. Which of the following solutions would be MOST effective for enforcing security policies on these personal mobile devices?

- (A) Installing antivirus software on each device

- (B) Establishing a separate guest Wi-Fi network for mobile devices
- (C) **Using Mobile Device Management (MDM) to enforce security policies**
- (D) Mandating that employees use strong passwords on their personal devices

Explanation 337. Correct Answer: C. Using Mobile Device Management (MDM) to enforce security policies. MDM solutions provide centralized control to enforce security policies, manage device features, and ensure that personal devices meet the organization's security standards before accessing corporate resources.

Option A is incorrect. While installing antivirus software is a good security measure, it doesn't provide the comprehensive policy enforcement capabilities that MDM does.

Option B is incorrect. A separate guest Wi-Fi may restrict access to the internal network, but it doesn't manage or enforce security policies on the devices themselves.

Option D is incorrect. While using strong passwords is essential, it's just one aspect of device security. MDM offers broader policy enforcement capabilities.

Question 338. David, an IT administrator, noticed an unusually high data usage on several company-owned mobile devices even when they are connected to the corporate Wi-Fi. He suspects these devices might be using cellular data in the background. Which of the following solutions should David

implement to ensure that company devices use only the corporate Wi-Fi for data transactions when they're in the office?

- (A) Enable Airplane mode on all devices
- (B) Set up a Wi-Fi whitelist
- (C) **Implement a mobile device management (MDM) policy to prioritize Wi-Fi**
- (D) Disable cellular antennas in the office area

Explanation 338. Correct Answer: C. Implement a mobile device management (MDM) policy to prioritize Wi-Fi. An MDM solution allows administrators to enforce policies on mobile devices. By implementing a policy that prioritizes Wi-Fi connections, David can ensure that company devices will use the corporate Wi-Fi network when available, thus reducing cellular data usage.

Option A is incorrect. While enabling Airplane mode would cut off cellular data, it would also disable all other forms of communication including Wi-Fi, making the device unusable for its intended purposes.

Option B is incorrect. Setting up a Wi-Fi whitelist does not prevent a device from using cellular data. It only restricts which Wi-Fi networks a device can connect to.

Option D is incorrect. Disabling cellular antennas is a drastic measure that could affect other devices and services in the vicinity. It's also impractical and potentially illegal depending on local regulations.

Question 339. A security team recently upgraded their intrusion detection system (IDS). Since the upgrade, the system hasn't flagged any intrusions, even though intrusion attempts are a regular occurrence. What is this situation best characterized as?

- (A) A true negative
- (B) **A false negative**
- (C) A true positive
- (D) A confirmation feedback

Explanation 339. Correct Answer: B. A false negative. A false negative occurs when a system fails to detect a threat or vulnerability that is actually present. In this scenario, the IDS isn't detecting real intrusion attempts, which could lead to undetected breaches.

Option A is incorrect. A true negative would mean that the system correctly identified that there were no intrusions when there truly weren't any. This isn't the scenario described as intrusion attempts are expected.

Option C is incorrect. A true positive means that the threat or vulnerability was correctly identified and truly exists. Since no intrusions are being detected, this isn't a true positive.

Option D is incorrect. "Confirmation feedback" isn't a standard term related to vulnerability detection and doesn't apply to the described scenario.

Question 340. XYZ Corporation is planning to deploy a new wireless infrastructure in their newly acquired office building. The IT manager wants to ensure optimal wireless coverage

throughout the premises. Which of the following should the IT team prioritize before installing the wireless access points?

- (A) Purchase the most expensive wireless access points to ensure maximum range
- (B) Conduct a site survey to determine the best locations for access points**
- (C) Deploy all access points near windows to enhance signal strength
- (D) Ensure all users have 5GHz capable devices

Explanation 340. Correct Answer: B. Conduct a site survey to determine the best locations for access points. A site survey will help identify the optimal placements for access points to achieve consistent and robust wireless coverage across the entire premises.

Option A is incorrect. While quality equipment is essential, the costliest access points might not always guarantee the best results. Placement and environment play crucial roles in wireless performance.

Option C is incorrect. Deploying access points near windows can cause signal leakage, potentially making the signal available outside the intended area and presenting a security risk.

Option D is incorrect. While ensuring users have 5GHz capable devices is a good practice, it doesn't relate directly to the optimal installation of wireless access points.

Question 341. XYZ Company uses MDM to manage company-owned and employee-owned mobile devices. An employee

reported losing their personal phone over the weekend. What MDM feature should the IT department use to ensure that sensitive company data on the lost phone isn't accessed?

- (A) Monitor the device's location
- (B) Force update the device's apps
- (C) **Remote wipe the device**
- (D) Change the user's email password

Explanation 341. Correct Answer: C. Remote wipe the device. Using the remote wipe feature, the IT department can erase all data, including company data, from the lost device, ensuring that sensitive information doesn't fall into the wrong hands.

Option A is incorrect. Monitoring the device's location might help in finding it but doesn't prevent unauthorized access to the data on the device.

Option B is incorrect. Force updating the device's apps might address vulnerabilities in the apps but doesn't directly protect the company data on the device.

Option D is incorrect. Changing the user's email password can prevent unauthorized access to the user's email, but it doesn't secure other sensitive company data that might be on the device.

Question 342. After a series of cyber incidents, AlphaTech Corp. wants to take proactive measures to identify vulnerabilities in their network. They aim to obtain a comprehensive report of potential weaknesses without exploiting them. Which of the following would best meet this

objective?

- (A) Penetration test
- (B) **Vulnerability scan**
- (C) Red team assessment
- (D) Port security

Explanation 342. Correct Answer: B. Vulnerability scan. A vulnerability scan is designed to inspect systems, networks, and applications to identify potential weaknesses or vulnerabilities. Unlike some of the other options, it doesn't attempt to exploit these vulnerabilities; it merely identifies and reports them.

Option A is incorrect. A penetration test goes a step further than a vulnerability scan. While it identifies vulnerabilities, it also attempts to exploit them to understand the potential impact of a breach.

Option C is incorrect. A red team assessment is a goal-based assessment where a simulated adversary (the red team) tries to achieve specific objectives. It often involves exploitation, which goes beyond the mere identification of vulnerabilities.

Option D is incorrect. Port security is a feature at the data link layer to control MAC address-based access on a port-by-port basis. It doesn't offer a comprehensive vulnerability report.

Question 343. GammaTech is in the final stages of deploying a new application. Before the deployment, the security team wants to examine the application's code without executing it to identify any potential vulnerabilities. Which vulnerability identification method should the team employ?

- (A) Penetration Testing
- (B) Dynamic Analysis
- (C) **Static Analysis**
- (D) Fuzz Testing

Explanation 343. Correct Answer: C. Static Analysis. Static analysis involves examining an application's code, bytecode, or binary code without executing it to identify vulnerabilities. This method allows security teams to find potential security issues in the codebase before the application runs.

Option A is incorrect. Penetration testing involves actively trying to exploit vulnerabilities in a system or application. It does not focus on code examination without execution.

Option B is incorrect. Dynamic analysis examines an application during its runtime, observing its behavior to identify vulnerabilities.

Option D is incorrect. Fuzz testing, or fuzzing, involves providing a program with a series of random inputs to see if any of them cause crashes or other unexpected behavior, helping identify vulnerabilities.

Question 344. During a routine vulnerability assessment, TechInc discovers a weakness in their system that, if exploited, would allow an attacker to modify existing user accounts, including privileges. Which classification best describes this vulnerability?

- (A) **Elevation of privilege vulnerability**
- (B) Disclosure vulnerability

- (C) Replay vulnerability
- (D) Remote code execution vulnerability

Explanation 344. Correct Answer: A. Elevation of privilege vulnerability. Elevation of privilege vulnerabilities allow attackers to increase their privileges within a system, often giving them more access than intended. The scenario describes a situation where user accounts and their privileges can be modified, aligning with this classification.

Option B is incorrect. Disclosure vulnerabilities involve unauthorized access to information but not the modification of user privileges or data.

Option C is incorrect. Replay vulnerabilities occur when attackers capture and later retransmit valid data transmissions to fool a system, which is not described in the given scenario.

Option D is incorrect. Remote code execution vulnerabilities allow attackers to execute arbitrary commands or code on a target system. While these can be severe, the given scenario specifically describes privilege changes, not arbitrary code execution.

Question 345. A healthcare organization uses embedded systems in various medical devices. They are aware of the potential threats these systems can pose if not properly secured. Which of the following is NOT a recommended practice when hardening embedded systems in this context?

- (A) Regularly patching and updating the firmware of the devices

- (B) Allowing unrestricted access to the devices for ease of use by the medical staff**
- (C) Disabling unnecessary services and features not required for the device's primary function**
- (D) Changing default credentials and using strong, unique passwords for device access**

Explanation 345. Correct Answer: B. Allowing unrestricted access to the devices for ease of use by the medical staff.

Unrestricted access can lead to unintentional or deliberate misconfigurations or misuse of the device, compromising its security.

Option A is incorrect. Regularly patching and updating firmware is a critical aspect of maintaining the security of embedded systems, especially with the evolving nature of threats.

Option C is incorrect. Disabling unnecessary services and features reduces the attack surface and is a fundamental principle of system hardening.

Option D is incorrect. Changing default credentials and ensuring strong, unique passwords are in place is essential to prevent unauthorized access.

Question 346. TechSoft Corp. is implementing a new asset-tracking system to monitor its vast array of computing resources. Which of the following should be the PRIMARY reason for maintaining an up-to-date hardware and software inventory?

- (A) To ensure software licenses are renewed on time
- (B) **To identify and respond to unauthorized devices or software promptly**
- (C) To aid in the procurement of new hardware and software
- (D) To provide employees with an understanding of available resources

Explanation 346. Correct Answer: B. To identify and respond to unauthorized devices or software promptly.

While all the options have valid reasons for maintaining an inventory, from a security standpoint, identifying unauthorized devices or software promptly is crucial. Unauthorized devices or software can pose a significant security risk, including potential data breaches or malware infections.

Option A is incorrect. While renewing software licenses is important, it's not the primary security reason for maintaining an inventory.

Option C is incorrect. Procurement decisions benefit from inventory data but do not directly impact immediate security concerns in the way that identifying unauthorized assets does.

Option D is incorrect. While providing employees with resource understanding is beneficial, it isn't as crucial for security as promptly identifying unauthorized assets.

Question 347. An enterprise is deploying IoT-based security cameras across multiple office locations. As the lead security professional, what recommendation would you prioritize to establish a secure baseline for these devices?

- (A) Setting the devices to public mode so all employees can access the feed for transparency
- (B) Regularly updating the device firmware to patch known vulnerabilities**
- (C) Enabling Universal Plug and Play (UPnP) to ensure easy connectivity for all devices on the network
- (D) Using the same password for all cameras for ease of management

Explanation 347. Correct Answer: B. Regularly updating the device firmware to patch known vulnerabilities. Regular firmware updates ensure that the IoT devices are protected against identified vulnerabilities, helping maintain their security posture.

Option A is incorrect. Setting devices to a public mode can lead to potential breaches of privacy and unauthorized access.

Option C is incorrect. UPnP can introduce vulnerabilities by automatically opening ports and allowing devices to set their configurations, potentially leading to security risks.

Option D is incorrect. Using the same password for all devices creates a single point of failure. If one device's password is compromised, all devices become vulnerable.

Question 348. A medium-sized enterprise is concerned about the security of its office workstations after a series of malware infections. As a security analyst, which of the following recommendations would BEST improve the security baseline of the workstations?

- (A) Install multiple antivirus solutions to ensure maximum detection
- (B) Set up screensavers with cyber hygiene tips to educate users
- (C) **Disable unnecessary services and ports on the workstations**
- (D) Frequently change the desktop wallpaper to prevent monotony

Explanation 348. Correct Answer: C. Disable unnecessary services and ports on the workstations. By disabling unnecessary services and ports, you reduce the number of potential attack vectors and vulnerabilities, thus improving the security baseline of the workstations.

Option A is incorrect. Installing multiple antivirus solutions can lead to conflicts and may degrade system performance. It's better to have one robust, updated antivirus solution.

Option B is incorrect. While cyber hygiene tips can be informative, they don't directly contribute to the technical security baseline of a workstation.

Option D is incorrect. Changing the desktop wallpaper does nothing for security. Its primary purpose is aesthetics.

Question 349. AlphaCorp is migrating to cloud infrastructure and wants to ensure all virtual machines (VMs) are securely configured from the onset. Before deploying multiple VM instances, what should AlphaCorp do to ensure each VM starts from a secure configuration?

- (A) Use the default VM templates provided by the cloud provider
- (B) Establish a secure baseline for VM configurations and use it for deployment**
- (C) Regularly backup all VMs
- (D) Use multi-factor authentication for cloud access

Explanation 349. Correct Answer: B. Establish a secure baseline for VM configurations and use it for deployment.

Establishing a secure baseline for VM configurations ensures that each VM is deployed with a set of standard security settings, reducing vulnerabilities from default configurations or potential misconfigurations.

Option A is incorrect. Relying solely on default VM templates provided by cloud providers may not meet the specific security requirements of an organization. Customizing and creating a secure baseline is more effective.

Option C is incorrect. While regular backups are essential for data recovery, they do not directly ensure that VMs start from a secure configuration.

Option D is incorrect. Multi-factor authentication is a crucial security measure for accessing cloud resources, but it doesn't ensure that VMs are deployed with secure configurations.

Question 350. A multinational company is deploying a new set of servers in its data centers across various countries. Which of the following steps should be taken FIRST to ensure the servers are secured against potential threats?

- (A) Set up a monitoring system to alert the IT team of any irregular activities
- (B) Deploy all the software applications the company might need in the future
- (C) Use the server's default configuration to ensure manufacturer's best practices are maintained
- (D) **Disable any unused services and ports on the server**

Explanation 350. Correct Answer: D. Disable any unused services and ports on the server. When setting up a new server, it's crucial to minimize its attack surface. Disabling unused services and ports ensures that only necessary services run on the server, reducing potential vulnerabilities.

Option A is incorrect. While monitoring is vital for security, before setting up a monitoring system, it's more crucial to harden the server to minimize vulnerabilities. Monitoring should complement hardening measures.

Option B is incorrect. Deploying all the software applications the company might need in the future can introduce unnecessary vulnerabilities and overhead. It's better to install only what's needed and keep the server lean.

Option C is incorrect. Relying on a server's default configuration can be risky, as it might not be tailored for an organization's specific needs and could have open ports or services that are unnecessary.

Question 351. While analyzing a vulnerability in a company's web application, the security team refers to a specific CVE to

understand the vulnerability's details. They further assess its CVSS score to decide on the remediation urgency. Which of the following best describes the purpose of the CVE and CVSS in this context?

- (A) CVE provides a severity score, while CVSS gives a unique identifier for the vulnerability
- (B) CVE and CVSS both offer a scoring mechanism to rank vulnerabilities
- (C) **CVE provides a unique identifier, while CVSS offers a standardized severity score**
- (D) CVE and CVSS are regulatory requirements for all software applications

Explanation 351. Correct Answer: C. CVE provides a unique identifier, while CVSS offers a standardized severity score. CVE (Common Vulnerabilities and Exposures) offers a standardized identifier for vulnerabilities, ensuring clear communication and reference. CVSS (Common Vulnerability Scoring System) provides a standardized method for rating the severity of vulnerabilities, enabling organizations to prioritize remediation.

Option A is incorrect. It's the opposite. CVE gives a unique identifier, while CVSS provides a severity score.

Option B is incorrect. Only CVSS offers a scoring mechanism to rank vulnerabilities. CVE offers unique identifiers.

Option D is incorrect. While using CVE and CVSS can be considered best practices, they aren't regulatory requirements for all software applications.

Question 352. The network administrator at a university wants to ensure that when students log onto the campus wireless network, their credentials are verified by the university's central authentication server. Additionally, the administrator wants to make sure that the data between the wireless access point and the central server is encrypted. Which solution should the administrator implement?

- (A) WPA3 with SAE
- (B) WPA2-Personal with AES
- (C) **WPA2-Enterprise with RADIUS**
- (D) Open wireless with VPN

Explanation 352. Correct Answer: C. WPA2-Enterprise with RADIUS. WPA2-Enterprise provides a more robust authentication method suitable for larger organizations like universities. By using RADIUS, the university can centralize the authentication process, ensuring students' credentials are verified against the central server. RADIUS also encrypts the data between the wireless access point and the central server, providing an additional layer of security.

Option A is incorrect. WPA3 with SAE is primarily used for secure handshakes between devices and does not directly relate to centralized authentication against a server like RADIUS.

Option B is incorrect. WPA2-Personal with AES is designed for personal or small office use where a pre-shared key is used. It doesn't support centralized authentication like RADIUS.

Option D is incorrect. While a VPN can encrypt data between a device and a network, it doesn't centralize wireless

authentication in the way that RADIUS does with WPA2-Enterprise.

Question 353. As part of the company's vulnerability management initiative, the security team has decided to conduct a series of penetration tests. Which of the following is the PRIMARY reason for incorporating penetration testing as a threat identification method?

- (A) To ensure compliance with regulatory requirements
- (B) To validate the efficiency of security awareness training
- (C) **To actively exploit vulnerabilities and assess potential impact**
- (D) To identify misconfigurations in the SIEM system

Explanation 353. Correct Answer: C. To actively exploit vulnerabilities and assess potential impact. Penetration testing is a method used to actively exploit vulnerabilities in an environment. Its primary purpose is to determine the potential impact and risk of those vulnerabilities in a real-world scenario, thereby allowing the organization to understand and prioritize remediation efforts.

Option A is incorrect. While some regulations might require penetration testing, the primary goal of the test is not just for compliance but to understand vulnerabilities' potential impact.

Option B is incorrect. Although penetration testing can sometimes be used to gauge the effectiveness of security training (for instance, in social engineering tests), it's not the primary reason for conducting these tests.

Option D is incorrect. SIEM systems are used for logging and event management. While a pen test might uncover misconfigurations in various systems, its primary purpose is not to focus on the SIEM.

Question 354. An organization has recently received a new software patch for its critical infrastructure. Before deploying it to production, the security team wants to understand its behavior and ensure it doesn't contain any malicious code. Which of the following methods would be MOST effective for safely executing and observing the patch's behavior?

- (A) Deploying the patch during a maintenance window
- (B) **Running the patch within a sandbox environment**
- (C) Conducting a code review of the patch
- (D) Installing the patch on a virtual machine

Explanation 354. Correct Answer: B. Running the patch within a sandbox environment. Running the patch within a sandbox environment allows the security team to execute and observe the software's behavior in an isolated environment, ensuring it doesn't interfere with or harm the actual production environment.

Option A is incorrect. Deploying the patch during a maintenance window reduces operational disruptions but doesn't allow for safe observation of the patch's behavior.

Option C is incorrect. While a code review can identify potential security concerns in the patch, it may not reveal the actual behavior when executed.

Option D is incorrect. Installing the patch on a virtual machine is a form of isolation, but a sandbox provides a more controlled and restrictive environment specifically designed for observing software behavior.

Question 355. GreenTech Inc. is selling a set of old servers to another company. Before the transaction, they want to ensure the data on these servers is irretrievable and they can prove that due diligence was performed. What should GreenTech seek to assure the buyer of proper data destruction?

- (A) A receipt of sale for the servers
- (B) A detailed log of the server's usage
- (C) **A certificate of data sanitization**
- (D) A user manual of the servers

Explanation 355. Correct Answer: C. A certificate of data sanitization. A certificate of data sanitization from a reputable entity provides assurance that all data on the servers was securely and completely wiped. Such certificates confirm that specific techniques were used to ensure data is irretrievable, giving confidence to the buyer.

Option A is incorrect. A receipt of sale only proves the transaction took place but does not address data sanitization or destruction.

Option B is incorrect. A log of the server's usage might detail its operational history but does not provide assurance of data destruction.

Option D is incorrect. A user manual provides instructions on how to use the server but does not address the state or security of the data it once held.

Question 356. Jane, the CISO at a financial institution, is overseeing the decommissioning of several old servers. She is aware that while some data must be destroyed, other data must be retained due to industry regulations. Which principle should Jane primarily focus on to ensure compliance?

- (A) Minimum necessary principle
- (B) Principle of least privilege
- (C) **Data retention policy**
- (D) Mandatory vacation policy

Explanation 356. Correct Answer: C. Data retention policy.

A data retention policy specifically defines how long data should be retained and the manner of its storage based on business needs, regulatory requirements, and other factors. In the context of decommissioning servers, adhering to this policy will ensure that Jane complies with regulations related to data retention.

Option A is incorrect. The minimum necessary principle pertains to healthcare and refers to only using, disclosing, or requesting the amount of information necessary to accomplish a specific task.

Option B is incorrect. The principle of least privilege pertains to access controls and means giving users the minimum levels of access necessary to perform their jobs.

Option D is incorrect. A mandatory vacation policy pertains to ensuring employees take time off so that potential fraudulent activities might be detected in their absence. It doesn't directly address data retention.

Question 357. CyberFirm, a leading software development company, recently updated their server OS due to new features and patches. Given that they have already established and deployed a secure baseline in the past, what should CyberFirm do NEXT to ensure continued security?

- (A) Conduct a complete system reboot for all servers
- (B) Re-deploy the same baseline without any modifications
- (C) **Update the secure baseline to include new configurations and then deploy it**
- (D) Implement a new firewall rule for the servers

Explanation 357. Correct Answer: C. Update the secure baseline to include new configurations and then deploy it.

When there are significant updates or changes to systems, it's crucial to review and update the secure baseline accordingly, ensuring it remains relevant and effective for the current environment. After updating the baseline, it should then be re-deployed.

Option A is incorrect. A complete system reboot does not address the maintenance of the secure baseline after an OS update.

Option B is incorrect. Simply re-deploying the same baseline without adjustments might miss out on specific configurations or considerations needed due to the OS update.

Option D is incorrect. While firewall rules are essential for security, they don't directly address the maintenance and updating of a secure baseline.

Question 358. MatrixCorp recently adopted a mobile strategy where employees are provided with company-owned devices. These devices are also allowed for personal use, but the organization retains the ability to manage and monitor them. Which deployment model is MatrixCorp using?

- (A) Bring Your Own Device (BYOD)
- (B) Choose Your Own Device (CYOD)
- (C) **Corporate-owned, Personally Enabled (COPE)**
- (D) Public Device Deployment (PDD)

Explanation 358. Correct Answer: C. Corporate-owned, Personally Enabled (COPE). The COPE model involves organizations providing employees with company-owned devices that they can also use for personal tasks. However, the company retains full control, management, and monitoring capabilities over these devices.

Option A is incorrect. In the BYOD model, employees use their personal devices for work, not company-provided ones.

Option B is incorrect. CYOD allows employees to select a device from a list of company-approved devices, but the emphasis is on choice rather than personal use of corporate-owned devices.

Option D is incorrect. Public Device Deployment (PDD) is not a recognized deployment model in the context of mobile solutions.

Question 359. A company has recently upgraded its wireless infrastructure and wants to ensure that the data transmitted over its wireless network is protected using the most recent and secure encryption standards. Which of the following should the company configure on its wireless access points?

- (A) WEP
- (B) WPA
- (C) WPA2
- (D) **WPA3**

Explanation 359. Correct Answer: D. WPA3. WPA3 is the latest iteration of Wi-Fi Protected Access, designed to improve upon the security features of WPA2. It offers enhanced protections against brute-force attacks, superior encryption methods, and a more secure handshake process.

Option A is incorrect. WEP (Wired Equivalent Privacy) is an outdated and insecure protocol that can be easily cracked. It should not be used for securing wireless networks.

Option B is incorrect. While WPA (Wi-Fi Protected Access) was a significant improvement over WEP, it has been surpassed by both WPA2 and WPA3 in terms of security features.

Option C is incorrect. WPA2 has been a strong standard for many years but has vulnerabilities that WPA3 addresses, making WPA3 the more secure option.

Question 360. A security analyst is exploring ways to proactively identify vulnerabilities within the organization's infrastructure. Which of the following provides the BEST method for the analyst to receive real-time threat intelligence from the dark web?

- (A) Utilizing a vulnerability scanner on the organization's internal network
- (B) **Subscribing to a dark web threat intelligence feed**
- (C) Conducting regular penetration tests on external-facing systems
- (D) Reviewing daily reports from the organization's SIEM system

Explanation 360. Correct Answer: B. Subscribing to a dark web threat intelligence feed. Threat intelligence feeds, especially those focusing on the dark web, provide real-time information about emerging threats and vulnerabilities. This proactive approach allows analysts to be aware of potential threats even before they may affect the organization.

Option A is incorrect. While vulnerability scanners are effective at identifying known vulnerabilities within a network, they don't provide real-time threat intelligence from external sources like the dark web.

Option C is incorrect. Penetration tests are indeed useful for identifying vulnerabilities in systems and applications. However, they don't specifically provide threat intelligence from the dark web.

Option D is incorrect. SIEM systems aggregate and analyze log data from various sources to identify and respond to security incidents. While they can alert to current threats within the environment, they don't offer real-time dark web threat intelligence.

Question 361. XYZ Corp is designing their new web application infrastructure. They want to ensure that all web traffic to and from their application is encrypted. In addition to selecting HTTPS as the protocol, which default port should they configure for this encrypted traffic?

- (A) 21
- (B) 80
- (C) 443
- (D) 25

Explanation 361. Correct Answer: C. 443. Port 443 is the default port used for HTTPS (HTTP over SSL/TLS) traffic. It ensures that web traffic is encrypted and provides a secure communication channel between the client and the server.

Option A is incorrect. Port 21 is the default port for FTP (File Transfer Protocol), which is used for transferring files, not encrypted web traffic.

Option B is incorrect. Port 80 is the default port for HTTP, which is unencrypted.

Option D is incorrect. Port 25 is the default port for SMTP (Simple Mail Transfer Protocol), which is used for email transmission, not encrypted web traffic.

Question 362. TechWorld Corp is concerned about cybercriminals sending emails that appear to come from its domain to deceive its clients. The company wants to implement a solution that would allow receiving email servers to validate that an email claiming to come from TechWorld Corp's domain indeed originates from an approved server. Which of the following should the company implement?

- (A) SMTP authentication
- (B) **DKIM**
- (C) POP3 over SSL
- (D) S/MIME

Explanation 362. Correct Answer: B. DKIM. DomainKeys Identified Mail (DKIM) is a method used to authenticate the origin and integrity of an email. With DKIM, a digital signature is added to the headers of outgoing emails. Receiving email servers then use this signature to validate the email by checking it against the sending domain's public key, which is published in the DNS records.

Option A is incorrect. SMTP authentication ensures that users provide valid credentials before they can send emails through a server, but it doesn't validate the domain of the sender to the receiver.

Option C is incorrect. POP3 over SSL (Secure Sockets Layer) is about securely retrieving email messages from a server. It doesn't provide a way to authenticate the sender's domain.

Option D is incorrect. S/MIME (Secure/Multipurpose Internet Mail Extensions) is used to encrypt and sign email messages.

While it ensures the integrity and confidentiality of the email content, it does not validate the sender's domain to the recipient.

Question 363. After a security incident, a forensic investigation revealed that a compromised internal workstation was communicating with a known malicious IP address. To prevent further communication, the security team decided to take immediate action. Which of the following is the BEST immediate action to ensure the workstation cannot communicate with that IP?

- (A) **Implement a block rule on the web filter for the IP address**
- (B) Disable the network port of the compromised workstation
- (C) Use a honeypot to divert the traffic from the malicious
- (D) Update the firewall's firmware

Explanation 363. Correct Answer: A. Implement a block rule on the web filter for the IP address. By implementing a block rule specifically for the known malicious IP address on the web filter, any attempt to communicate with that IP would be stopped, effectively preventing further malicious communications.

Option B is incorrect. Disabling the network port of the compromised workstation would disconnect the machine from the network, but it wouldn't specifically prevent communication with the malicious IP if the port were to be re-enabled.

Option C is incorrect. While honeypots can be used to divert or study attacker behavior, they are not the most direct way to block communication with a known malicious IP address.

Option D is incorrect. Updating the firewall's firmware is a general maintenance task and does not specifically address blocking communications with the known malicious IP.

Question 364. Amy, a network administrator, is researching tools to assist with automating the evaluation of her organization's systems against a specific security baseline. She comes across SCAP and wants to implement it. Which of the following BEST describes the primary function of the Security Content Automation Protocol (SCAP)?

- (A) To facilitate the real-time transfer of threat intelligence feeds
- (B) To provide an interface for user authentication against Active Directory
- (C) **To allow for automated vulnerability management and policy compliance evaluation**
- (D) To offer encrypted communication channels for remote system management

Explanation 364. Correct Answer: C. To allow for automated vulnerability management and policy compliance evaluation. SCAP (Security Content Automation Protocol) is a suite of open standards that enhances the ability of organizations to automate vulnerability management, measurement, and policy compliance evaluation on systems.

Option A is incorrect. While threat intelligence is crucial for security, SCAP is not designed primarily for real-time threat intelligence feed transfers.

Option B is incorrect. SCAP does not directly deal with user authentication against any directory services.

Option D is incorrect. SCAP's primary function isn't to offer encrypted communication channels for remote system management. Other protocols and tools serve this purpose.

Question 365. A pharmaceutical company is working on a new drug formula that promises to revolutionize the treatment of a particular disease. The R&D team has detailed documentation on the components, procedures, and results of the drug trials. How should this documentation be classified to ensure that only the right people within the company have access?

- (A) Implement a Domain Name System (DNS) firewall
- (B) Employ URL scanning to identify and block malicious URLs**
- (C) Rely on manual reporting of suspicious URLs by employees
- (D) Use a Virtual Private Network (VPN) to redirect all employee web traffic

Explanation 365. Correct Answer: B. Employ URL scanning to identify and block malicious URLs. URL scanning can identify potentially malicious sites by examining the complete URL and comparing it with known malicious URLs or patterns. This method can block access to URLs that are designed to look similar to legitimate ones.

Option A is incorrect. While a DNS firewall can help block access to malicious domains, URL scanning provides more granular control by examining the full URL, not just the domain.

Option C is incorrect. Relying solely on manual reporting by employees may not be as efficient or effective as an automated URL scanning solution. It would also place undue responsibility on employees to recognize and report every malicious URL.

Option D is incorrect. Using a VPN simply changes the route of the traffic and provides encrypted communication. It does not inherently offer URL scanning or filtering capabilities.

Question 366. A financial institution wants to ensure that any unauthorized access to customer data triggers an immediate alert to the security team. Which of the following approaches would be the MOST effective in achieving this requirement?

- (A) Configure alerts for any modification to database records
- (B) Set up alerts for successful logins during off-business hours
- (C) **Establish alerting thresholds based on anomalous user behavior**
- (D) Send daily reports of all access attempts to the security team for review

Explanation 366. Correct Answer: C. Establish alerting thresholds based on anomalous user behavior. By setting alerting thresholds based on anomalous behavior, the system can detect unauthorized access based on patterns that deviate

from typical user behavior, providing timely alerts for potential breaches.

Option A is incorrect. Configuring alerts for any modification to database records may generate a high number of false positives, especially in a dynamic environment like a financial institution where legitimate changes occur regularly.

Option B is incorrect. While setting up alerts for off-hours access can catch some unauthorized attempts, it might miss breaches occurring during business hours.

Option D is incorrect. Daily reports may delay the detection and response to unauthorized access, as it doesn't offer real-time alerting.

Question 367. A marketing team is collaborating on a new campaign and requires access to a shared folder. However, they shouldn't be able to modify files created by others. How should permissions be set on this shared folder?

- (A) Assign the marketing team full control
- (B) Allow the marketing team read-only access
- (C) Assign the marketing team write-only access
- (D) **Assign the marketing team modify permission but deny the delete permission**

Explanation 367. Correct Answer: D. Assign the marketing team modify permission but deny the delete permission. By providing modify permissions but denying delete permissions, team members can create and edit their own files, but they won't be able to delete or modify files created by others.

Option A is incorrect. Full control would allow team members to modify or delete any file, which is not desired.

Option B is incorrect. Read-only access would prevent team members from creating or editing any files.

Option C is incorrect. Write-only access would prevent team members from viewing existing files in the folder.

Question 368. Alice, a cybersecurity analyst, is tasked with identifying potential weaknesses in a newly deployed web application's infrastructure before it goes live. She wants a tool that can proactively discover and report on system vulnerabilities, missing patches, and misconfigurations. Which of the following should Alice utilize for this purpose?

- (A) Intrusion Detection System (IDS)
- (B) Network sniffer
- (C) **Vulnerability scanner**
- (D) Security Information and Event Management (SIEM) system.

Explanation 368. Correct Answer: C. Vulnerability scanner.

Vulnerability scanners are designed to discover and report potential vulnerabilities in systems by probing and analyzing them. They can detect issues such as missing patches, misconfigurations, and known software flaws.

Option A is incorrect. An IDS detects and alerts on potential malicious activities based on specific signatures or heuristics but does not proactively scan for vulnerabilities.

Option B is incorrect. A network sniffer captures and analyzes network traffic but does not perform vulnerability assessments on infrastructure components.

Option D is incorrect. While a SIEM system can aggregate and analyze log and event data from various sources, it does not proactively scan for vulnerabilities like a vulnerability scanner.

Question 369. Globex Industries is expanding its data centers across multiple geographic locations. The IT team wants to have a centralized system to get real-time status, outages, and metrics of all data center infrastructures. Which of the following solutions would be the MOST effective for this purpose?

- (A) Data Loss Prevention (DLP) tools
- (B) Distributed Denial of Service (DDoS) protection
- (C) Security Information and Event Management (SIEM)
- (D) **Infrastructure Management Platform (IMP)**

Explanation 369. Correct Answer: D. Infrastructure Management Platform (IMP). IMPs provide centralized control and monitoring for infrastructure across multiple sites. They deliver insights into infrastructure health, outages, and metrics, ensuring that the IT team can address issues promptly.

Option A is incorrect. DLP tools focus on preventing unauthorized data transfers and exfiltrations, not on monitoring infrastructure health and status.

Option B is incorrect. DDoS protection tools safeguard against denial-of-service attacks but aren't designed to monitor the overall health or metrics of data center infrastructures.

Option C is incorrect. While SIEM solutions centralize log data and provide insights into security events, they are not designed primarily to monitor data center infrastructure health across multiple locations.

Question 370. The IT department of XYZ Corp is keen on preventing users from changing specific system settings, such as altering the firewall configurations. The majority of their infrastructure is based on Windows operating systems. Which of the following would be the most effective way to achieve this?

- (A) Use SELinux to enforce strict access controls
- (B) Utilize Group Policy to set and enforce policies related to system settings**
- (C) Deploy a third-party software solution to lock system settings
- (D) Implement a user training program to guide users on system settings best practices

Explanation 370. Correct Answer: B. Utilize Group Policy to set and enforce policies related to system settings. Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. This can be used to enforce specific policies related to system settings in a Windows environment.

Option A is incorrect. SELinux (Security-Enhanced Linux) is primarily used in Linux environments to enforce mandatory access controls. It wouldn't be appropriate for a primarily Windows-based infrastructure.

Option C is incorrect. While third-party solutions may exist, leveraging built-in features like Group Policy is often more streamlined, cost-effective, and efficient.

Option D is incorrect. While user training is essential, relying solely on training without implementing technical controls is not effective in preventing users from altering system settings.

Question 371. A company plans to upgrade its email server to ensure that email transmission between their mail server and client applications is encrypted. Which of the following protocols would be the most appropriate for this purpose?

- (A) HTTP
- (B) FTP
- (C) **IMAP over SSL/TLS**
- (D) SNMP

Explanation 371. Correct Answer: C. IMAP over SSL/TLS.

IMAP over SSL/TLS (commonly known as IMAPS) is a protocol used by email clients to retrieve messages from a mail server over a secure channel. The use of SSL/TLS provides encryption for the transmitted data, ensuring confidentiality of the email transmission.

Option A is incorrect. HTTP is a protocol for transferring web content and does not provide encryption by default. Furthermore, it's not designed for email transmission.

Option B is incorrect. FTP is a protocol for transferring files and does not provide secure email transmission capabilities.

Option C is incorrect. SNMP (Simple Network Management Protocol) is used for network management and monitoring, not for email transmission.

Question 372. Lisa, a security administrator, is using a popular benchmark to ensure the web servers in her organization are configured securely. She wants to make sure that unnecessary services are disabled, and appropriate permissions are set. Which of the following organizations is MOST likely the source of the benchmark she is using?

- (A) PCI DSS
- (B) OWASP
- (C) CIS
- (D) GDPR

Explanation 372. Correct Answer: C. CIS. The Center for Internet Security (CIS) is known for its CIS Benchmarks, which provide prescriptive guidance for configuring systems securely.

Option A is incorrect. PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

Option B is incorrect. OWASP (Open Web Application Security Project) is known for its top ten list of web application vulnerabilities and not for system configuration benchmarks.

Option D is incorrect. GDPR (General Data Protection Regulation) is a regulation that requires businesses to protect

the personal data and privacy of EU citizens. It doesn't provide benchmarks for secure system configurations.

Question 373. The IT department at TechCorp Ltd has been instructed to ensure that critical system files remain unchanged to avoid potential security breaches. They want to implement a system that can provide alerts whenever there is an unauthorized change to these files. Which of the following would best serve this purpose?

- (A) Data Loss Prevention (DLP)
- (B) Intrusion Detection System (IDS)
- (C) **File Integrity Monitoring (FIM)**
- (D) Remote Monitoring and Management (RMM)

Explanation 373. Correct Answer: C. File Integrity Monitoring (FIM). File Integrity Monitoring (FIM) tools monitor and detect changes in files that may indicate a breach, malware infection, or other unauthorized activity. By tracking and reporting on file change patterns, FIM helps ensure the integrity and confidentiality of data.

Option A is incorrect. Data Loss Prevention (DLP) focuses on preventing unauthorized data transfers or leaks from the organization, not on monitoring file changes.

Option B is incorrect. An Intrusion Detection System (IDS) primarily detects unauthorized access or attacks on a network. While it can identify some unauthorized file changes, it isn't specifically designed for file integrity monitoring.

Option D is incorrect. Remote Monitoring and Management (RMM) tools primarily allow IT professionals to monitor and manage endpoints, networks, and computers remotely. They don't specifically focus on file integrity.

Question 374. ABC Tech has a mixed environment with both Linux and Windows servers. They want to ensure that processes running on their Linux servers only have access to specific resources and are restricted from performing certain actions. Which of the following tools would be most appropriate for this task?

- (A) Use Group Policy on their Windows servers and apply it to Linux servers
- (B) Implement a strict user training regimen to inform users about security best practices
- (C) **Enable Security-Enhanced Linux (SELinux) in enforcing mode**
- (D) Limit user access to Linux servers

Explanation 374. Correct Answer: C. Enable Security-Enhanced Linux (SELinux) in enforcing mode. SELinux provides mandatory access controls by limiting the actions a process can perform to only those defined in its policy, ensuring it only has access to specific resources. By setting SELinux in enforcing mode, these policies are actively enforced.

Option A is incorrect. Group Policy is specific to Windows and cannot be applied directly to Linux servers.

Option B is incorrect. While user training is a good security practice, it does not provide the technical control required to restrict processes on Linux servers.

Option D is incorrect. Limiting user access to Linux servers does not directly control the actions of processes running on those servers.

Question 375. Sarah, a security administrator, is implementing a monitoring solution for her organization's server infrastructure. She wants a solution that does not require any additional software to be installed on the servers themselves. Which type of monitoring approach should Sarah choose?

- (A) Agent-based monitoring
- (B) Intrusion Detection System (IDS)
- (C) **Agentless monitoring**
- (D) Network-based Application Performance Monitoring (APM)

Explanation 375. Correct Answer: C. Agentless monitoring.

Agentless monitoring solutions do not require any software agents to be installed on the servers they monitor. They typically rely on standard protocols and interfaces to collect performance and other data.

Option A is incorrect. Agent-based monitoring requires the installation of software agents on each server or device that is to be monitored.

Option B is incorrect. While an Intrusion Detection System (IDS) is a security tool, it is not specifically designed for agentless infrastructure monitoring.

Option D is incorrect. Network-based Application Performance Monitoring (APM) is focused on monitoring application performance on the network, not on agentless server monitoring.

Question 376. PharmaCorp, a pharmaceutical company, wants to ensure that its researchers cannot transfer proprietary formulas and research data to external storage devices or cloud storage. The company needs a solution to prevent such transfers while allowing other types of data to be transferred. What should they implement?

- (A) Web Application Firewall (WAF)
- (B) Data Encryption Tool
- (C) **Data Loss Prevention (DLP)**
- (D) Virtual Private Network (VPN)

Explanation 376. Correct Answer: C. Data Loss Prevention (DLP). Data Loss Prevention (DLP) is designed to detect potential data breach attempts and prevent the unauthorized transfer of sensitive data. By setting up rules and criteria in a DLP solution, PharmaCorp can restrict the transfer of proprietary information while allowing other data to be transferred as needed.

Option A is incorrect. A Web Application Firewall (WAF) is used to protect web applications by filtering and monitoring

HTTP traffic. It does not handle data transfers to external storage or cloud storage specifically.

Option B is incorrect. A Data Encryption Tool encrypts data to protect it from unauthorized access. While it adds a layer of security, it doesn't prevent the transfer of data to external devices or cloud storage.

Option D is incorrect. A Virtual Private Network (VPN) provides a secure tunnel for data transmission between two endpoints. It does not prevent or monitor the type of data being transferred.

Question 377. CyberFirm has been facing issues with phishing campaigns where attackers spoof their domain to send fraudulent emails. They already implemented DKIM to sign their emails but want an additional measure to specify which mail servers are authorized to send emails on behalf of their domain. Which security measure should CyberFirm adopt?

- (A) SPF
- (B) PGP
- (C) SSL certificate
- (D) IMAP

Explanation 377. Correct Answer: A. SPF. Sender Policy Framework (SPF) is designed to prevent email spoofing. It allows domain owners to specify which mail servers are authorized to send emails on behalf of their domain. Receiving servers can then verify the sending server against the SPF record in the domain's DNS.

Option B is incorrect. PGP (Pretty Good Privacy) is used for encrypting and decrypting texts, emails, files, directories, and whole disk partitions, but it doesn't define authorized mail servers for a domain.

Option C is incorrect. An SSL certificate provides a secure connection between a user's web browser and a website, ensuring data confidentiality. It's not specifically designed to validate the sending mail servers of a domain.

Option D is incorrect. IMAP (Internet Message Access Protocol) is a protocol used by email clients to retrieve messages from a mail server. It doesn't help in specifying authorized mail servers for a domain.

Question 378. A school wants to prevent its students from accessing inappropriate websites during class hours. The IT department decides to implement a solution that blocks requests to specific domain names associated with inappropriate content. Which of the following security solutions would best address this need?

- (A) Firewall filtering based on IP addresses
- (B) Intrusion Detection System monitoring
- (C) Virtual Private Network (VPN) enforcement
- (D) **DNS filtering with a blacklist**

Explanation 378. Correct Answer: D. DNS filtering with a blacklist. DNS filtering is a technique that can be used to prevent users from accessing specific websites by blocking requests to certain domain names. A blacklist can be created to list the domain names associated with inappropriate content,

and when users try to access these sites, the DNS filter will not resolve the domain name, thereby preventing access.

Option A is incorrect. While firewalls can block traffic based on IP addresses, this method is not as effective for blocking specific domain names, especially when a domain can have multiple IP addresses or if the IPs can change.

Option B is incorrect. Intrusion Detection Systems (IDS) are primarily used for detecting and alerting on malicious activities but not for blocking access to specific domain names.

Option C is incorrect. VPNs are used to create a secure communication channel and are not inherently designed to block domain name resolutions.

Question 379. A large financial institution recently experienced a security breach where an attacker was able to bypass its intrusion detection system (IDS). Upon investigation, the security team found out that the attacker utilized a zero-day exploit. In the aftermath, what should the institution do to enhance the capability of its IDS?

- (A) **Switch from a signature-based IDS to a behavior-based IDS**
- (B) Disable the IDS and rely solely on firewall rules
- (C) Update the IDS with the latest threat intelligence feeds and signatures
- (D) Reduce the frequency of IDS signature updates

Explanation 379. Correct Answer: A. Switch from a signature-based IDS to a behavior-based IDS. Behavior-

based IDS (or anomaly-based IDS) monitors network traffic and compares it against an established baseline, allowing it to potentially detect zero-day exploits and other novel attacks that signature-based systems might miss.

Option B is incorrect. Relying solely on firewall rules without IDS would lessen the security depth and expose the institution to more risks.

Option C is incorrect. While updating the IDS with the latest signatures is important, it wouldn't necessarily detect zero-day exploits until a signature for that exploit has been created and disseminated.

Option D is incorrect. Reducing the frequency of IDS signature updates would make the system even more vulnerable to recent threats.

Question 380. A security analyst at CyberSecure Corp. reviews a vulnerability report concerning an application that could allow attackers to upload malicious scripts. Once these scripts are executed, they can grant attackers complete control over the application. How should this vulnerability be primarily classified?

- (A) Integrity vulnerability
- (B) Availability vulnerability
- (C) **Remote code execution vulnerability**
- (D) Disclosure vulnerability

Explanation 380. Correct Answer: C. Remote code execution vulnerability. Remote code execution (RCE)

vulnerabilities allow attackers to run arbitrary commands or scripts on a targeted system. In the scenario, the application vulnerability grants attackers the ability to upload and execute malicious scripts, which aligns with this classification.

Option A is incorrect. While the vulnerability can affect the integrity of the application, the primary concern here is the ability of attackers to execute code remotely, making it an RCE vulnerability.

Option B is incorrect. Availability vulnerabilities primarily concern the disruption of services or systems, preventing authorized users from accessing them. The scenario doesn't indicate any disruption of availability.

Option D is incorrect. Disclosure vulnerabilities involve unauthorized viewing or accessing of information. The described vulnerability goes beyond mere disclosure, allowing execution of malicious scripts.

Question 381. After a recent security incident in the organization, the IT team noticed that several legitimate activities were being flagged by the intrusion detection system, resulting in a high number of false positives. What is the MOST appropriate action to improve the system's accuracy and reduce unnecessary alerts?

- (A) Disable the intrusion detection system for a week to observe regular network traffic patterns
- (B) Set up a stricter firewall rule to block all external traffic
- (C) **Implement alert tuning to refine the system's**

detection criteria

(D) Encourage employees to reduce their internet usage

Explanation 381. Correct Answer: C. Implement alert tuning to refine the system's detection criteria. Alert tuning involves adjusting the detection rules or criteria of a system to better differentiate between legitimate and malicious activities, thereby reducing false positives.

Option A is incorrect. Disabling the intrusion detection system can expose the organization to real threats, making it a risky approach.

Option B is incorrect. Setting up stricter firewall rules doesn't directly address the issue of false positives from the intrusion detection system and could block legitimate business operations.

Option D is incorrect. Reducing internet usage does not necessarily correlate with a decrease in false positives. The issue lies with the system's criteria, not the amount of traffic.

Question 382. ABC Corp has recently faced a security breach due to a contractor connecting an infected laptop to the corporate network. Management wants to implement a solution that would ensure that any device connecting to the corporate network meets the company's security standards, including up-to-date antivirus definitions. Which solution should ABC Corp consider?

(A) Intrusion Detection System (IDS)

(B) Virtual Private Network (VPN)

- (C) Network Access Control (NAC)
- (D) Web Application Firewall (WAF)

Explanation 382. Correct Answer: C. Network Access Control (NAC). Network Access Control (NAC) allows organizations to set policies for device connectivity to corporate networks. NAC can assess the security posture of a device before it connects to ensure it meets predefined criteria, such as updated antivirus definitions, required patches, etc.

Option A is incorrect. An Intrusion Detection System (IDS) monitors network traffic for suspicious activities and issues alerts but does not evaluate device security postures before allowing network access.

Option B is incorrect. A Virtual Private Network (VPN) allows secure remote access to a network but does not inherently evaluate the security posture of devices.

Option D is incorrect. A Web Application Firewall (WAF) focuses on protecting web applications by monitoring and filtering HTTP traffic. It is not used for evaluating device security postures.

Question 383. Global Corp received a report that some of its customers received phishing emails that seemed to originate from the company's domain. The IT team checked and confirmed that SPF and DKIM configurations were correctly set. What additional email security measure can Global Corp implement to provide clear policies on how the emails should be treated if they don't align with SPF and DKIM?

- (A) Enabling TLS encryption
- (B) **Implementing DMARC policies**
- (C) Setting up a new SMTP server
- (D) Increasing email retention period

Explanation 383. Correct Answer: B. Implementing DMARC policies. By implementing DMARC policies, Global Corp can define how email receivers should handle emails from its domain that don't align with the specified SPF and DKIM records. DMARC can be set to monitor, quarantine, or reject emails that fail these checks, providing more robust protection against email spoofing and phishing.

Option A is incorrect. While TLS encryption is essential for protecting the content of email in transit, it doesn't address the issue of spoofing or provide guidelines on how to handle emails that don't match SPF and DKIM.

Option C is incorrect. Setting up a new SMTP server can help with sending emails, but it doesn't inherently protect against email spoofing or provide guidance for emails that don't align with SPF and DKIM.

Option D is incorrect. Increasing the email retention period affects how long emails are stored but doesn't offer protection against spoofing or guidance for handling misaligned emails.

Question 384. A financial firm has just experienced a cyber attack, and the IT team identified a piece of malware that evaded their traditional antivirus solutions. The CISO now wants to not only detect but also be able to analyze and respond

to such advanced threats in real-time. Which solution should the firm consider implementing?

- (A) Vulnerability Scanner
- (B) Intrusion Prevention System (IPS)
- (C) **Endpoint Detection and Response (EDR)**
- (D) Patch Management System

Explanation 384. Correct Answer: C. Endpoint Detection and Response (EDR). Endpoint Detection and Response (EDR) provides real-time monitoring and analysis of endpoint events, allowing an organization to detect, investigate, and respond to potential security threats. EDR tools can identify behaviors that might indicate advanced threats that evade traditional antivirus solutions.

Option A is incorrect. Vulnerability Scanners are used to identify vulnerabilities in a system or network but do not provide real-time monitoring and response capabilities for threats.

Option B is incorrect. Intrusion Prevention Systems (IPS) monitor network traffic to prevent potential threats, but they might not provide in-depth analysis and response at the endpoint level like EDR solutions do.

Option D is incorrect. Patch Management Systems are used to manage the distribution and installation of software updates but do not offer real-time threat detection and response.

Question 385. After the recent cyber-attack on Acme Corp, the IT security team decided to enhance their proactive defense

mechanism. They want to start with identifying unpatched and vulnerable systems on their network. Which of the following scanning activities would BEST assist them in this endeavor?

- (A) Conducting a passive scan during business hours
- (B) Implementing a full open port scan on all systems
- (C) **Running a credentialed vulnerability scan on their network**
- (D) Scanning the external perimeter for domain name resolutions

Explanation 385. Correct Answer: C. Running a credentialed vulnerability scan on their network. A credentialed vulnerability scan uses valid user credentials to access and scan the target system, allowing for a deeper and more comprehensive check for vulnerabilities, including unpatched systems.

Option A is incorrect. A passive scan is non-intrusive and only monitors network traffic, limiting its capability to identify unpatched systems actively.

Option B is incorrect. While a full open port scan can identify open ports, it doesn't necessarily identify unpatched systems or specific vulnerabilities.

Option D is incorrect. Scanning the external perimeter for domain name resolutions can help in gathering information about domain names but won't directly assist in identifying unpatched systems.

Question 386. A software developer in a company notices that a legitimate software tool they use is repeatedly flagged and quarantined by the company's security solution. Which of the following is the BEST action the cybersecurity team can take to address this without compromising security?

- (A) Turn off the antivirus solution
- (B) **Whitelist the software tool in the antivirus settings**
- (C) Decrease the security level of the antivirus
- (D) Install a different antivirus solution

Explanation 386. Correct Answer: B. Whitelist the software tool in the antivirus settings. Whitelisting allows the cybersecurity team to specify software or applications that are considered safe and should not be flagged or quarantined by the antivirus solution.

Option A is incorrect. Turning off the antivirus solution would leave the system vulnerable to malware and other malicious threats.

Option C is incorrect. Decreasing the security level of the antivirus might reduce its effectiveness in detecting and blocking genuine threats.

Option D is incorrect. Simply installing a different antivirus solution does not guarantee that the tool won't be flagged again, and frequent switches can also be costly and time-consuming.

Question 387. AlphaTech, a growing SaaS company, has multiple applications deployed across different cloud providers. The security team struggles to manage and analyze logs from

these disparate sources. Which solution would BEST help AlphaTech centralize their logs for a more streamlined analysis?

- (A) Network Intrusion Detection System (NIDS)
- (B) **Log Aggregation Tool**
- (C) Data Loss Prevention (DLP) software
- (D) Vulnerability Scanner

Explanation 387. Correct Answer: B. Log Aggregation Tool.

Log aggregation tools are specifically designed to gather, centralize, and manage logs from various sources, making it easier to analyze and correlate events.

Option A is incorrect. While a NIDS can help detect malicious activity on a network, it doesn't centralize logs from different application sources.

Option C is incorrect. DLP software focuses on preventing unauthorized data transfers and does not serve the purpose of centralizing logs.

Option D is incorrect. Vulnerability Scanners are designed to identify vulnerabilities in a system but don't aggregate logs from various sources.

Question 388. BetaTech, a tech manufacturing firm, wants to ensure that a potential compromise of its IoT devices will not endanger its primary manufacturing control systems. Which of the following approaches would be most effective in achieving this?

- (A) Using a single robust firewall for the entire network
- (B) Periodic password changes for IoT devices

- (C) **Segmenting the IoT devices from the manufacturing control systems**
- (D) Enabling automatic updates for all IoT devices

Explanation 388. Correct Answer: C. Segmenting the IoT devices from the manufacturing control systems. By segmenting the IoT devices from the primary manufacturing control systems, BetaTech ensures that a compromise of the IoT devices doesn't immediately put the control systems at risk. Segmentation acts as a barrier to restrict the potential spread of malicious activity.

Option A is incorrect. While a robust firewall is crucial for network security, it does not replace the need for segmentation, especially with varied devices and risk profiles.

Option B is incorrect. Although periodic password changes can enhance the security of IoT devices, it does not prevent a compromised IoT device from affecting other parts of the network.

Option D is incorrect. Automatic updates can fix known vulnerabilities in IoT devices, but they don't provide the isolation that segmentation offers to prevent a compromise from affecting other network segments.

Question 389. A global manufacturing company wants to ensure its employees worldwide do not access websites promoting hate speech, gambling, or explicit content during working hours. To meet this requirement, which web filtering technique would be the most efficient?

- (A) Deploy a centralized proxy with location-based filtering
- (B) Use a blacklist of specific URLs known to contain such content
- (C) **Implement content categorization and block undesired categories**
- (D) Monitor internet usage logs and reprimand violators

Explanation 389. Correct Answer: C. Implement content categorization and block undesired categories. Content categorization is a technique where websites are categorized based on their content type, such as “gaming,” “social media,” “news,” etc. By using this technique, organizations can block entire categories of content, such as “hate speech” or “gambling,” ensuring broad coverage without the need to identify every problematic URL individually.

Option A is incorrect. While centralized proxies can help manage internet access, location-based filtering focuses more on geographic locations rather than content categories.

Option B is incorrect. Relying solely on a blacklist can be inefficient, as it requires constant updates to catch every possible harmful URL, and it might not cover newly created sites quickly enough.

Option D is incorrect. Simply monitoring internet usage logs and reprimanding violators is reactive and does not proactively prevent access to undesired content.

Question 390. TechCo, a medium-sized enterprise, is planning to implement a solution to monitor, control, and restrict web

access for its employees to improve productivity and enhance security. They also want to cache frequently accessed web content to reduce bandwidth consumption. Which solution would BEST fit TechCo's requirements?

- (A) Deploy a decentralized proxy on each departmental network
- (B) Set up a DNS-based filtering service
- (C) **Use a centralized proxy with caching capabilities**
- (D) Recommend browser extensions for web filtering to all employees

Explanation 390. Correct Answer: C. Use a centralized proxy with caching capabilities. A centralized proxy allows organizations to filter, monitor, and control web access from a central point. Additionally, proxies with caching capabilities can store frequently accessed web content, reducing the need for repeated downloads and thus saving bandwidth.

Option A is incorrect. A decentralized approach would make it challenging to consistently apply and enforce policies across the enterprise. It may also lead to inefficiencies in bandwidth usage as content caching would not be centralized.

Option B is incorrect. While a DNS-based filtering service can help in blocking access to certain malicious or inappropriate sites, it does not offer the centralized control or caching capabilities that a proxy does.

Option D is incorrect. Relying on browser extensions is a decentralized method that depends on user compliance and may not provide centralized control or caching capabilities.

Question 391. An organization is planning to deploy a new web application that will be accessible from both the internal network and the internet. The application will communicate exclusively over HTTPS. The security administrator is asked to configure the firewall to allow the necessary traffic. Which of the following should the administrator configure?

- (A) Allow port 21 and block all others
- (B) **Allow port 443 and block all others**
- (C) Allow port 80 and block all others
- (D) Allow port 23 and block all others

Explanation 391. Correct Answer: B. Allow port 443 and block all others. HTTPS primarily uses port 443 for secure communication. Thus, allowing port 443 and blocking all others would ensure the secure operation of the web application.

Option A is incorrect. Port 21 is used for FTP (File Transfer Protocol), which is not relevant to HTTPS communication.

Option C is incorrect. While port 80 is used for HTTP, it does not provide the encryption that HTTPS does on port 443.

Option D is incorrect. Port 23 is used for Telnet, which is unrelated to secure web communication.

Question 392. The company's security administrator observes that there are multiple unauthorized access attempts originating from IP addresses in a specific range. The administrator wants to prevent these IP addresses from accessing the corporate network temporarily. Which of the following firewall configurations would BEST address this requirement?

- (A) **Configure an implicit deny rule for the specific IP range**
- (B) Set up a honeypot for the specific IP range
- (C) Allow the IP range but set a bandwidth limit
- (D) Add the IP range to a whitelist

Explanation 392. Correct Answer: A. Configure an implicit deny rule for the specific IP range. By configuring an implicit deny rule for that specific IP range, the firewall will block any traffic from those addresses, preventing them from accessing the network.

Option B is incorrect. While a honeypot can be used to monitor and analyze attacker behavior, it does not block the access of the specified IP range to the corporate network.

Option C is incorrect. Allowing the IP range and setting a bandwidth limit would not prevent access; it would only restrict the amount of data they could send/receive.

Option D is incorrect. Adding the IP range to a whitelist would grant them access, which is opposite to the required action.

Question 393. The IT department of Globex Corp is concerned about the increasing number of malicious websites being accessed from company laptops while employees are working remotely. They want to ensure that the web filter policies set in the corporate network are enforced even when devices are offsite. What would be the BEST solution to address this concern?

- (A) Implement a cloud-based web filtering solution

- (B) Use a VPN to force all remote traffic through the corporate network
- (C) **Deploy an agent-based web filter on all company laptops**
- (D) Periodically send reminders to employees about acceptable web usage

Explanation 393. Correct Answer: C. Deploy an agent-based web filter on all company laptops. Agent-based web filters can enforce web filtering policies on a device regardless of its location. This ensures that the policies apply consistently whether the device is on or off the corporate network.

Option A is incorrect. While cloud-based solutions can offer offsite filtering, they might not be as consistent as an agent-based solution that directly enforces corporate policies on the device itself.

Option B is incorrect. Using a VPN would force all traffic through the corporate network, which could cause latency and might not be feasible for all remote work scenarios.

Option D is incorrect. Sending reminders is a passive approach and may not effectively prevent access to malicious websites.

Question 394. Lisa, a cybersecurity analyst, is setting up a centralized system to correlate logs from multiple sources, detect malicious activities in real-time, and produce comprehensive security reports. Which tool should Lisa consider for this purpose?

- (A) Network Intrusion Detection System (NIDS)

- (B) Web Application Firewall (WAF)
- (C) Vulnerability Scanner
- (D) **Security Information and Event Management (SIEM)**

Explanation 394. Correct Answer: D. Security Information and Event Management (SIEM). SIEM tools are designed to aggregate, correlate, and analyze logs and events from various sources in an organization. They help in detecting and responding to security incidents in real-time and generating detailed security reports.

Option A is incorrect. While NIDS monitors and analyzes network traffic for signs of malicious activities, it doesn't provide centralized logging and reporting functionalities like a SIEM.

Option B is incorrect. A Web Application Firewall (WAF) protects web applications from web-based attacks. It does not offer the centralized log correlation and analysis features of a SIEM.

Option C is incorrect. A Vulnerability Scanner identifies vulnerabilities in systems and applications but doesn't aggregate and analyze logs from various sources.

Question 395. Lucy, the IT security manager of a financial company, receives an automated alert that an employee attempted to email a document containing social security numbers to an external email address. Which of the following tools most likely generated this alert?

- (A) Network Intrusion Detection System (NIDS)
- (B) **Data Loss Prevention (DLP) solution**
- (C) Vulnerability Scanner
- (D) Packet Analyzer

Explanation 395. Correct Answer: B. Data Loss Prevention (DLP) solution. DLP solutions are specifically designed to monitor and control data transfers across an organization's network. In this case, the DLP detected sensitive data—social security numbers—being sent outside of the organization and alerted Lucy.

Option A is incorrect. NIDS detects and alerts on malicious activity on a network, but it doesn't typically scan for specific data types being transferred.

Option C is incorrect. Vulnerability scanners identify and report on vulnerabilities in a system but don't monitor data transfers.

Option D is incorrect. While packet analyzers can capture and analyze network traffic, they don't inherently generate alerts based on the specific content of data being transferred.

Question 396. An online banking platform wants to improve its customer verification process when users open a new account. Which of the following identity proofing methods would be the MOST secure for this purpose?

- (A) Asking users to select a security question and answer from a list
- (B) **Requiring users to upload a photo of a government-**

issued ID and a selfie

- (C) Sending a verification code to the user's email address
- (D) Prompting users to provide their favorite color

Explanation 396. Correct Answer: B. Requiring users to upload a photo of a government-issued ID and a selfie. This method provides a high level of assurance by comparing a user's live image (selfie) with a government-issued ID. The combination ensures the person is who they claim to be.

Option A is incorrect. Security questions, especially from a pre-defined list, can be easily guessed or obtained by attackers.

Option C is incorrect. Verification codes via email can enhance identity proofing but aren't as robust as checking against a government ID and selfie.

Option D is incorrect. Personal preferences, like favorite colors, are weak indicators of identity and can be easily guessed.

Question 397. A company has recently noticed an increased number of employees accessing social media sites during work hours, leading to decreased productivity. To counter this, the security administrator decides to limit access to these websites during peak working hours. Which firewall rule modification should the administrator make?

- (A) Implement an Intrusion Prevention System (IPS) rule to block social media content
- (B) **Change the firewall rule to deny access to known social media IP addresses between 9 AM and 5 PM**

- (C) Use the firewall's URL filtering capability to blacklist social media URLs
- (D) Increase the firewall's bandwidth to accommodate the excess traffic

Explanation 397. Correct Answer: B. Change the firewall rule to deny access to known social media IP addresses between 9 AM and 5 PM. Implementing a time-based rule that denies access to specific IP addresses (or ranges) associated with social media can be an effective way to restrict access during specified hours.

Option A is incorrect. An IPS is designed to detect and prevent malicious activities based on signatures. Blocking social media content is not typically its primary function.

Option C is incorrect. URL filtering would block access to the URLs entirely. The requirement is to block them only during specific hours.

Option D is incorrect. Increasing the firewall's bandwidth doesn't address the problem of employees accessing social media during work hours.

Question 398. A company wants to host a public-facing website but ensure that even if the website gets compromised, attackers cannot gain access to sensitive internal data. Which of the following is the BEST configuration to achieve this?

- (A) Place the web server on the internal network and strictly monitor the traffic
- (B) Place the web server in the DMZ with a firewall in

front of it and another firewall between the DMZ and the internal network

(C) Directly connect the web server to the internet without a firewall and move sensitive data off the server

(D) Place the web server in the DMZ and connect it directly to the internal network without a firewall

Explanation 398. Correct Answer: B. Place the web server in the DMZ with a firewall in front of it and another firewall between the DMZ and the internal network. By placing the web server in a DMZ, and having two firewalls (one facing the internet and another facing the internal network), the company can ensure that even if the public-facing web server is compromised, the attacker would still need to bypass another firewall to reach the internal network.

Option A is incorrect. Placing a public-facing web server on the internal network, even with monitoring, exposes the network to unnecessary risks.

Option C is incorrect. Connecting a server directly to the internet without any form of firewall is highly risky, even if sensitive data is moved.

Option D is incorrect. Without a firewall between the DMZ and the internal network, it becomes much easier for a compromised server in the DMZ to impact or access the internal network.

Question 399. A Security Analyst at BetaTech is reviewing the monitoring tools deployed across the organization. She wants to

ensure that every tool can detect unauthorized changes made to system files and configurations. Which of the following tools is BEST suited for this purpose?

- (A) Network protocol analyzer
- (B) **File integrity monitoring (FIM) system**
- (C) Bandwidth monitoring tool
- (D) Passive vulnerability scanner

Explanation 399. Correct Answer: B. File integrity monitoring (FIM) system. File integrity monitoring systems are designed to detect and alert when unauthorized changes are made to system files and configurations, ensuring the integrity of these critical components.

Option A is incorrect. While network protocol analyzers can capture and analyze network traffic, they are not specifically designed to monitor changes to system files and configurations.

Option C is incorrect. Bandwidth monitoring tools primarily track network usage and bandwidth consumption, not modifications to system files.

Option D is incorrect. Passive vulnerability scanners monitor network traffic to detect vulnerabilities but do not actively track changes to system files.

Question 400. A company has noticed an increase in malware infections over the past month. After investigating, it was determined that the infections were caused by employees visiting websites that were newly registered but had malicious intent. Which of the following would be the BEST approach to

mitigate this threat?

- (A) Implement a block rule to deny access to all websites
- (B) **Use a web filter that incorporates domain reputation checks and blocks domains registered recently**
- (C) Set the web filter to block all websites not categorized as "Business"
- (D) Enforce multi-factor authentication for all internet-based applications

Explanation 400. Correct Answer: B. Use a web filter that incorporates domain reputation checks and blocks domains registered recently. Reputation-based web filters can evaluate the trustworthiness of domains. One common heuristic is to be suspicious of newly registered domains, as cybercriminals often use these for phishing or malware distribution.

Option A is incorrect. Blocking access to all websites is an extreme measure that would hinder business operations and employee productivity.

Option C is incorrect. Simply blocking websites not categorized as “Business” does not specifically target the threat of newly registered malicious domains. Additionally, some business-relevant websites might not be categorized properly.

Option D is incorrect. While multi-factor authentication can enhance security, it does not address the threat of employees visiting malicious websites.

Question 401. At AlphaTech, the security team is assessing vulnerabilities in a newly deployed cloud infrastructure. While

analyzing potential risks, they consider factors such as the physical location of data centers, local laws and regulations, and natural disaster frequencies. What are these considerations known as in the context of vulnerability management?

- (A) Asset valuation factors
- (B) Risk response variables
- (C) Threat intelligence variables
- (D) **Environmental variables**

Explanation 401. Correct Answer: D. Environmental variables. Environmental variables in vulnerability management refer to external factors that can influence or affect the security posture of an organization. These can include physical location, local laws and regulations, and the potential for natural disasters.

Option A is incorrect. Asset valuation factors primarily deal with determining the value of an asset to the organization and don't typically consider external factors like local laws or natural disaster frequencies.

Option B is incorrect. Risk response variables pertain to the organization's strategies and actions to respond to identified risks rather than the external factors influencing risk.

Option C is incorrect. Threat intelligence variables revolve around information regarding potential threats or threat actors. They don't typically encompass physical environment considerations like those described in the scenario.

Question 402. Caroline, a security analyst, receives an alert that an unfamiliar file has been detected on a mission-critical server. She suspects it might be malware. What is the BEST immediate action Caroline should take regarding this potential threat?

- (A) Delete the file immediately to prevent further damage
- (B) Quarantine the file to prevent it from executing or spreading**
- (C) Make a copy of the file for further analysis
- (D) Notify all employees about the suspicious file

Explanation 402. Correct Answer: B. Quarantine the file to prevent it from executing or spreading. Quarantining suspicious files isolates them, preventing potential execution or spread while allowing further investigation without immediate deletion.

Option A is incorrect. While deleting the file seems proactive, it removes the chance for further analysis and can affect forensic investigations.

Option C is incorrect. Making a copy is important for analysis, but the immediate priority should be to prevent potential execution or spread of the suspicious file. Quarantine first, then analyze.

Option D is incorrect. Notifying all employees about a specific suspicious file may cause panic or confusion. It's more appropriate to manage the incident first and then communicate relevant information in a structured manner.

Question 403. Jennifer, an IT administrator, is asked to onboard a new remote employee for a sales role. Which of the following is the BEST approach for provisioning the user account?

- (A) Assign the new user the same access privileges as the CEO because they might require all resources
- (B) Provide the new user with administrative rights to ensure they can install and configure any needed software
- (C) **Use the access privileges from a template of a salesperson to provide the required resources**
- (D) Allow the new user to decide and self-select the necessary access based on their job role

Explanation 403. Correct Answer: C. Use the access privileges from a template of a salesperson to provide the required resources. Provisioning users based on role templates ensures that users have just the access they need, adhering to the principle of least privilege.

Option A is incorrect. This goes against the principle of least privilege and can introduce significant security risks.

Option B is incorrect. Giving administrative rights to employees without a proper need can expose the organization to unnecessary risks.

Option D is incorrect. Users should not self-select access rights as they might not be aware of potential security implications.

Question 404. AlphaTech, a leading IT company, recently identified a critical vulnerability in its primary software product.

They have developed a patch to address the vulnerability. Before distributing the patch to its customers, which of the following should AlphaTech ideally perform?

- (A) Deploy the patch on all company systems
- (B) Notify the media about the vulnerability
- (C) **Test the patch in a controlled environment**
- (D) Offer compensation to affected customers

Explanation 404. Correct Answer: C. Test the patch in a controlled environment. Before deploying or distributing a patch, especially for a critical vulnerability, it's essential to test it in a controlled environment. This ensures that the patch doesn't introduce new issues and that it effectively addresses the vulnerability.

Option A is incorrect. Deploying the patch immediately on all company systems without testing it could lead to unforeseen issues or even exacerbate the problem.

Option B is incorrect. Notifying the media about the vulnerability, especially before it's been effectively addressed and without a coordinated disclosure plan, can lead to panic and potential exploitation by malicious actors.

Option D is incorrect. Offering compensation is reactive and doesn't directly address the vulnerability. The primary goal after identifying a vulnerability should be to address and mitigate it.

Question 405. After a major security incident, DeltaTech implemented several security patches to address vulnerabilities in their infrastructure. To ensure the effectiveness of these

patches, what should be DeltaTech's primary next step?

- (A) Deploy additional firewalls at the network perimeter
- (B) Provide cybersecurity training to all employees
- (C) **Rescan the systems to check if vulnerabilities are effectively addressed**
- (D) Change all user passwords across the organization

Explanation 405. Correct Answer: C. Rescan the systems to check if vulnerabilities are effectively addressed. After implementing security patches, it's essential to rescan the systems to ensure that the identified vulnerabilities have been effectively addressed and the patches have been implemented correctly.

Option A is incorrect. While firewalls are crucial for security, deploying them is not directly related to validating the effectiveness of newly implemented patches.

Option B is incorrect. Cybersecurity training for employees is vital, but it doesn't directly validate the success of the applied patches.

Option D is incorrect. Changing user passwords can be a necessary step after a breach, but it doesn't validate if the patches have successfully addressed vulnerabilities.

Question 406. An e-commerce company is rolling out a new web application to facilitate online payments. The IT department wants to be immediately notified of any application errors or unauthorized modifications to the application's codebase. Which of the following tools should they implement?

- (A) Web Application Firewall (WAF)
- (B) **Application Performance Monitoring (APM)**
- (C) Domain Name System (DNS) monitoring tool
- (D) Network flow analyzer

Explanation 406. Correct Answer: B. Application Performance Monitoring (APM). APM tools are designed to monitor the performance of applications and can detect application errors, anomalies, and unauthorized code changes, thereby ensuring application stability and security.

Option A is incorrect. While a WAF protects web applications from various cyber threats by filtering and monitoring HTTP traffic, it doesn't typically monitor for application errors or unauthorized code changes.

Option C is incorrect. DNS monitoring tools focus on ensuring the availability and integrity of DNS services and do not monitor application performance or codebase changes.

Option D is incorrect. Network flow analyzers examine data flows on the network but do not specifically monitor application performance or codebase modifications.

Question 407. Paul, a network administrator, has configured various networking devices in his organization to send alerts in the event of specific failures. After a switch experienced a power supply failure, Paul received an immediate notification. Which of the following did Paul most likely utilize to receive this notification?

- (A) Syslog server

- (B) Simple Network Management Protocol (SNMP) traps
- (C) Packet sniffer
- (D) Firewall logs

Explanation 407. Correct Answer: B. Simple Network Management Protocol (SNMP) traps. SNMP traps are unsolicited alert messages sent by a device to notify an SNMP management station of specific events. In this case, the switch sent an SNMP trap to Paul when it detected the power supply failure.

Option A is incorrect. While a Syslog server can be used to collect logs from various devices, it doesn't proactively send alerts based on specific events like an SNMP trap does.

Option C is incorrect. A packet sniffer captures and analyzes network traffic but doesn't actively alert administrators to specific device events.

Option D is incorrect. Firewall logs are specific to firewalls and track traffic that passes through the firewall, but they don't typically send unsolicited alerts about network device health.

Question 408. DeltaCorp, a retail company, has assessed that a security breach might result in a loss of \$1 million in sales. The company has determined that they can tolerate a loss of up to \$500,000, but anything beyond that would severely impact operations. To cover the potential financial loss beyond their tolerance level, they decide to purchase cybersecurity insurance. Which of the following terms best describes the \$500,000

figure?

- (A) Risk appetite
- (B) **Risk threshold**
- (C) Risk capacity
- (D) Risk assessment

Explanation 408. Correct Answer: B. Risk threshold. The risk threshold is the specific level of risk an organization is willing to accept. In this case, DeltaCorp is willing to accept potential losses up to \$500,000, marking that as their threshold.

Option A is incorrect. Risk appetite is a broader term that reflects the general level of risk an organization is willing to accept in pursuit of its objectives. It's more about strategic intent than specific figures.

Option C is incorrect. Risk capacity refers to the total amount of risk an organization can absorb without significantly impacting its strategic objectives or viability. It's a broader measure than the specific tolerance threshold.

Option D is incorrect. Risk assessment is the process of identifying, analyzing, and evaluating risks. It's not a specific figure or threshold.

Question 409. Samantha, a security analyst, has been tasked with creating a monthly report for senior management detailing the security posture of the company. Which of the following is the MOST important element to include to ensure the report effectively communicates the company's current security status?

- (A) Detailed technical logs of all security incidents

- (B) **Graphical representation of incidents by category**
- (C) A complete list of all users and their access levels
- (D) Copies of recent phishing emails for demonstration

Explanation 409. Correct Answer: B. Graphical representation of incidents by category. A graphical representation by category allows senior management to quickly understand the types and frequency of security incidents, which can help in decision-making and resource allocation.

Option A is incorrect. While technical logs are crucial for incident analysis, they may be too detailed and technical for a senior management report.

Option C is incorrect. While it's essential to manage user access levels, a complete list of all users and their access might be excessive for a monthly senior management report focused on the company's security posture.

Option D is incorrect. While examples of phishing emails can be educational, they are not crucial for a monthly report meant to provide an overview of the company's security status.

Question 410. After a recent security incident, Sarah, a network security analyst, wants to analyze the flow data of network traffic to identify patterns and potential threats. She wants to collect metadata about IP traffic flow and gather details like IP addresses, ports, and protocols used. Which tool should Sarah employ to obtain this information?

- (A) Intrusion Detection System (IDS)
- (B) Syslog server

- (C) NetFlow collector
- (D) Simple Network Management Protocol (SNMP) traps

Explanation 410. Correct Answer: C. NetFlow collector.

NetFlow is a network protocol developed by Cisco for collecting IP traffic information and monitoring network traffic. A NetFlow collector can provide insights into traffic flow patterns and volume, making it suitable for Sarah's requirements.

Option A is incorrect. While an IDS can provide alerts on malicious activities based on specific signatures or heuristics, it does not provide detailed flow data analysis like NetFlow.

Option B is incorrect. A Syslog server is mainly used for collecting and storing log data from various devices. It does not focus on detailed network traffic flow like NetFlow.

Option D is incorrect. SNMP traps are for sending unsolicited alert messages from a device to a management station regarding specific events. They don't provide traffic flow analysis.

Question 411. A security analyst has been tasked with investigating a possible data breach. While reviewing the network logs, the analyst noticed an unusual increase in outbound traffic to an unfamiliar IP address during non-business hours. The traffic appears to be encrypted and is associated with a known server containing sensitive data. Which of the following is the MOST likely explanation for this behavior?

- (A) The server is downloading patches
- (B) An employee is accessing the server remotely

- (C) A backup of the server is being performed
- (D) **Data exfiltration is occurring**

Explanation 411. Correct Answer: D. Data exfiltration is occurring. Given that the traffic is encrypted, associated with a sensitive server, and is being sent to an unfamiliar IP during non-business hours, the most likely scenario is that unauthorized data is being taken out of the network, which is known as data exfiltration.

Option A is incorrect. While servers do download patches, these are usually inbound traffic from a known update source, not outbound to unfamiliar IPs.

Option B is incorrect. While employees might access servers remotely, the traffic being encrypted and sent during non-business hours to an unfamiliar IP makes this less likely.

Option C is incorrect. Backups generally don't result in encrypted outbound traffic to unfamiliar IP addresses, especially during non-business hours.

Question 412. ExamsDigest Enterprises wants to streamline their permission assignments. They decide that rather than assigning permissions to each user individually, they will group users based on departmental roles and then assign permissions to these groups. For example, all members of the "Marketing" role would have access to the marketing database. Which access control method is ExamsDigest Enterprises employing?

- (A) Rule-based access control
- (B) **Mandatory Access Control (MAC)**

- (C) Discretionary Access Control (DAC)
- (D) **Role-Based Access Control (RBAC)**

Explanation 412. Correct Answer: D. Role-Based Access Control (RBAC). RBAC involves grouping users based on roles (in this case, departments like “Marketing”) and then assigning permissions to these roles. Individuals are then placed into these roles, which determines their access. The scenario described by ExamsDigest Enterprises is a clear example of implementing RBAC.

Option A is incorrect. Rule-based access control often deals with predefined rules for access, commonly used in firewalls or routers, and is not about grouping users based on roles.

Option B is incorrect. MAC is more about classifying information and having users with the appropriate clearance levels. It doesn’t deal with departmental roles like the scenario mentioned.

Option C is incorrect. DAC allows resource owners to grant or deny permissions. It does not inherently involve assigning permissions based on roles or job functions.

Question 413. BetaTech is implementing a new authentication mechanism for its data center technicians. Instead of using key cards, technicians will now have to look into a device that maps a specific pattern to authenticate their identity. Which of the following is BetaTech likely implementing?

- (A) Password system
- (B) **Retina scanning**

- (C) Hardware token
- (D) Knowledge-based questions

Explanation 413. Correct Answer: B. Retina scanning.

Retina scanning is a biometric method that analyzes the unique patterns of a person's retina to authenticate their identity. It's categorized under the "something you are" factor as it relies on a unique physical characteristic.

Option A is incorrect. A password system pertains to the "something you know" factor since users need to remember their passwords to authenticate.

Option C is incorrect. A hardware token represents the "something you have" factor, as it's a device the user needs to possess.

Option D is incorrect. Knowledge-based questions, such as "What's the name of your first pet?", fall under the "something you know" factor.

Question 414. A global financial company experiences sporadic cyber attacks on its infrastructure. The company notices that attacks that occur during non-business hours often result in more significant damage due to delayed responses. Which of the following measures would BEST decrease the reaction time to these off-hour attacks?

- (A) Train the security staff to handle larger volumes of incidents during business hours

- (B) Implement an automated intrusion detection and response system**
- (C) Increase the number of security staff during non-business hours**
- (D) Send email notifications to security personnel when attacks are detected**

Explanation 414. Correct Answer: B. Implement an automated intrusion detection and response system. By implementing an automated intrusion detection and response system, the company can ensure that attacks are detected and responded to in real-time, regardless of when they occur. This drastically reduces the reaction time compared to manual interventions.

Option A is incorrect. Training staff to handle more incidents during business hours doesn't address the issue of delayed responses during non-business hours.

Option C is incorrect. Increasing staff during non-business hours may help, but it might not be as efficient or cost-effective as automation, and there's still potential for human delay.

Option D is incorrect. Sending email notifications might still lead to delays, especially if staff is not checking emails promptly during off-hours.

Question 415. A digital forensics investigator has just concluded an investigation regarding a potential insider threat. Before presenting the findings to the organization's board, which of the following should the investigator ensure about the

forensic report?

- (A) The report includes technical jargon to showcase the depth of the investigation
- (B) The report emphasizes the investigator's credentials and experience
- (C) **The report provides a clear, concise summary of findings without unnecessary technical details**
- (D) The report contains detailed logs of every action taken by the investigator

Explanation 415. Correct Answer: C. The report provides a clear, concise summary of findings without unnecessary technical details. A forensic report's primary purpose is to convey the results of an investigation in a clear and understandable manner, especially to non-technical stakeholders. By avoiding unnecessary technical jargon and providing a concise summary, it ensures that the report's findings are accessible to all intended readers.

Option A is incorrect. While the depth of an investigation is important, inundating a report with technical jargon can make it difficult for non-technical individuals, such as board members, to understand the findings.

Option B is incorrect. While the investigator's credentials and experience might be important, they should not be the emphasis of the report. The focus should remain on the investigation's findings and their implications.

Option D is incorrect. While maintaining a detailed log of every action taken is crucial for the investigator's records and

ensuring the integrity of the investigation, including every detail in the report can be overwhelming and detract from its main findings.

Question 416. MegaCorp is transitioning to a cloud-based infrastructure and wants to allow its employees to access multiple cloud services without re-entering their credentials every time. They currently have an on-premises LDAP directory in place. Which approach should MegaCorp take to provide a seamless authentication experience?

- (A) MegaCorp should abandon their LDAP directory and create individual accounts for each cloud service
- (B) Integrate their LDAP with a Single Sign-On (SSO) solution that supports cloud services**
- (C) Store passwords in a plaintext file for users to access and login to cloud services manually
- (D) Force users to change passwords every day to enhance security across all cloud platforms

Explanation 416. Correct Answer: B. Integrate their LDAP with a Single Sign-On (SSO) solution that supports cloud services. By integrating the on-premises LDAP with an SSO solution, MegaCorp can leverage its existing user directory to authenticate and provide access to multiple cloud services without requiring users to log in separately for each service.

Option A is incorrect. Abandoning the existing LDAP directory would negate the benefits of central management and create administrative overhead.

Option C is incorrect. Storing passwords in plaintext is a significant security risk and goes against best practices.

Option D is incorrect. Forcing users to change passwords daily is impractical, could result in weaker passwords, and doesn't provide a seamless authentication experience.

Question 417. At ExamsDigest, employees can access the company's cloud-based storage system. However, access to certain files within the storage is determined by the employee's department, job title, and years of service. For instance, senior managers in the finance department with more than five years of service can view the company's financial forecasts. Which access control model is ExamsDigest using?

- (A) Rule-Based Access Control (RAC)
- (B) Role-Based Access Control (RBAC)
- (C) **Attribute-Based Access Control (ABAC)**
- (D) Discretionary Access Control (DAC)

Explanation 417. Correct Answer: C. Attribute-Based Access Control (ABAC). Attribute-Based Access Control (ABAC) determines access based on attributes of the user, resource, and environment. In the scenario, the employee's department, job title, and years of service are the attributes that determine their access to specific files.

Option A is incorrect. RAC works based on predefined rules, typically without involving multiple user attributes like department or job title.

Option B is incorrect. While RBAC is close in functionality, it assigns permissions based on roles (like “manager” or “clerk”), not on a combination of attributes.

Option D is incorrect. DAC allows resource owners to specify who can access their resources based on their discretion. It doesn’t involve a combination of attributes to determine access.

Question 418. You are an IT security professional for a large corporation. After receiving reports about some users being unable to access external websites, you decided to review the firewall logs. Which of the following would be a PRIMARY indicator in the logs that a rule is blocking outbound traffic?

- (A) Multiple entries of the same external IP address being ALLOWED
- (B) Timestamps showing large gaps between entries
- (C) **Entries showing DROP/REJECT action for outbound traffic to port 80 and 443**
- (D) Logs showing inbound traffic from multiple unknown external IP addresses

Explanation 418. Correct Answer: C. Entries showing DROP/REJECT action for outbound traffic to port 80 and 443. Port 80 and 443 are standard ports for HTTP and HTTPS respectively, which are commonly used for accessing websites. If users are unable to access external websites, it would make sense to check for DROP or REJECT actions for these ports in the firewall logs.

Option A is incorrect. If an external IP address is being ALLOWED multiple times, it wouldn't be the cause of users being unable to access websites.

Option B is incorrect. Large gaps between timestamps in logs can indicate various issues, but they aren't a direct indicator of a specific rule blocking outbound traffic.

Option D is incorrect. While inbound traffic from unknown IP addresses might be of concern, it doesn't specifically indicate an outbound traffic rule blocking users from accessing websites.

Question 419. DeltaCorp has a password policy in place which mandates users to change their passwords every 30 days.

However, some users complain that this results in them choosing simpler passwords or writing them down to remember them. How can DeltaCorp maintain security while addressing these concerns?

(A) Reduce the password change frequency but introduce more complexity requirements

(B) Eliminate password changes and rely solely on two-factor authentication

(C) Ask users to change passwords every week to improve security

(D) Allow users to reuse any of their last three passwords to ease the transition

Explanation 419. Correct Answer: A. Reduce the password change frequency but introduce more complexity requirements. By reducing the frequency of password changes, users are less burdened with the task of remembering new

passwords frequently. Adding complexity requirements can compensate for the longer duration by ensuring that passwords are strong.

Option B is incorrect. Relying solely on two-factor authentication (2FA) without any password requirements can introduce risks if the 2FA method is compromised. Additionally, 2FA can be inconvenient for users if not implemented correctly.

Option C is incorrect. Asking users to change passwords even more frequently would exacerbate the issue and likely lead to even weaker password practices.

Option D is incorrect. Allowing users to reuse recent passwords undermines the purpose of having them change passwords in the first place and reduces overall security.

Question 420. During a review of IDS logs, a security specialist notices a series of alerts indicating that a single external IP has been sending payloads that exploit a known vulnerability. However, the internal system to which these payloads are sent is patched and is not vulnerable to the exploit. Which of the following describes this type of IDS alert?

- (A) False positive
- (B) False negative
- (C) **True positive**
- (D) True negative

Explanation 420. Correct Answer: C. True positive. A true positive means the IDS correctly identified malicious or anomalous traffic. In this case, even though the internal system

isn't vulnerable, the IDS correctly flagged the traffic because it's genuinely malicious.

Option A is incorrect. A false positive would mean the IDS incorrectly flagged benign traffic as malicious, which is not the case here.

Option B is incorrect. A false negative means the IDS failed to identify malicious or anomalous traffic, but in this scenario, the IDS did correctly identify the malicious traffic.

Option D is incorrect. A true negative means the IDS correctly identified benign traffic as benign. The traffic in this scenario was malicious, so this doesn't apply.

Question 421. A popular social media platform allows third-party applications to access user data and post on behalf of users. To avoid sharing user passwords with third-party applications and provide limited, scoped access, which authentication method should the platform use?

- (A) Embed user passwords in the application's code
- (B) Use basic authentication with username and password for every request
- (C) **Implement Single Sign-On (SSO) using OAuth to provide token-based access**
- (D) Rely solely on CAPTCHA for third-party app authentication

Explanation 421. Correct Answer: C. Implement Single Sign-On (SSO) using OAuth to provide token-based access. OAuth provides token-based access and lets third-party

applications operate on behalf of users without exposing user passwords. OAuth tokens can also be scoped to limit the range of actions a third-party application can perform.

Option A is incorrect. Embedding passwords in application code is insecure and goes against best practices.

Option B is incorrect. Basic authentication exposes user credentials and doesn't offer the scoped access OAuth provides.

Option D is incorrect. CAPTCHA is designed to differentiate between human and automated access but doesn't handle authentication or authorization.

Question 422. An IT department in a large corporation spends several hours each day manually deploying patches and updates to thousands of workstations. Which of the following solutions would BEST enhance the efficiency of this process and save time for the IT team?

- (A) Disable automatic updates and conduct monthly patching sessions
- (B) **Implement an automated patch management system**
- (C) Designate a dedicated team for patching that operates in shifts
- (D) Educate users to install updates on their own

Explanation 422. Correct Answer: B. Implement an automated patch management system. By implementing an automated patch management system, the IT department can streamline the deployment of patches and updates across all

workstations, ensuring consistency, reducing manual efforts, and saving valuable time.

Option A is incorrect. Disabling automatic updates and conducting monthly patching sessions does not address the inefficiency of manual patching and might expose the systems to vulnerabilities for a longer time.

Option C is incorrect. While designating a dedicated team might distribute the workload, it doesn't eliminate the inefficiencies associated with manual patching.

Option D is incorrect. Relying on users to install updates introduces inconsistency, potential delays, and additional risks, as not all users might have the technical knowledge or remember to update regularly.

Question 423. An international company, GlobalTech, is using several web applications hosted by different vendors. To ensure their employees can access these applications without having to remember multiple sets of credentials, they want to implement a solution that can securely exchange user authentication information between the company and the service providers. What should GlobalTech implement?

- (A) Integrate each application with an independent LDAP server
- (B) **Implement SSO using Security Assertions Markup Language (SAML)**
- (C) Embed encrypted user credentials within the URL of each application

(D) Rely on public API keys shared between the company and each vendor

Explanation 423. Correct Answer: B. Implement SSO using Security Assertions Markup Language (SAML). SAML is an XML-based standard for exchanging authentication and authorization data between parties. It's designed to facilitate single sign-on for web applications. By implementing SSO with SAML, GlobalTech can allow its employees to authenticate once and gain access to multiple applications without re-authenticating.

Option A is incorrect. Having independent LDAP servers for each application defeats the purpose of SSO and complicates user management.

Option C is incorrect. Embedding encrypted user credentials in URLs is insecure and not a recommended practice.

Option D is incorrect. API keys are used for system-to-system communication and not for user authentication. Moreover, public API keys shouldn't be shared recklessly.

Question 424. A company wants to implement a solution that verifies the software integrity of remote servers before allowing them to connect to the primary network. Which of the following solutions BEST achieves this objective through attestation?

- (A)** Host-based firewall
- (B)** Whitelisting application
- (C)** **Remote attestation**
- (D)** VPN tunneling

Explanation 424. Correct Answer: C. Remote attestation.

Remote attestation is a process where a device (like a server) proves to a remote entity (like a network controller) that it is running genuine, unmodified software. It allows for the verification of the software integrity of remote devices before they connect to a primary network.

Option A is incorrect. A host-based firewall is used to control inbound and outbound network traffic to and from a device based on a set of configurable rules. It does not verify the software integrity of the device itself.

Option B is incorrect. A whitelisting application only allows specified software to run on a system. While it can enhance security by ensuring only approved software runs, it does not attest to the state or integrity of the device or its software when connecting to another network.

Option D is incorrect. VPN tunneling encrypts the connection between two points over the internet. While it ensures secure communication, it doesn't verify the software integrity of devices.

Question 425. TechCorp is collaborating with SoftTech, a business partner. To streamline collaboration without managing multiple accounts, TechCorp wants its employees to use their existing credentials to access SoftTech's online project management system. Which of the following approaches would BEST enable this functionality?

(A) TechCorp should create new accounts for its employees on SoftTech's system

- (B) SoftTech should allow anonymous access for TechCorp's employees
- (C) **TechCorp should implement federation between its identity provider and SoftTech's service provider**
- (D) SoftTech should reset all passwords and provide them to TechCorp's employees

Explanation 425. Correct Answer: C. TechCorp should implement federation between its identity provider and SoftTech's service provider. Federation allows two organizations to trust each other's identity systems. TechCorp's employees can use their existing credentials to access services on SoftTech's system without the need to create new accounts.

Option A is incorrect. Creating new accounts for every user in a collaborating organization isn't scalable and negates the advantages of federation.

Option B is incorrect. Allowing anonymous access would compromise security and wouldn't guarantee identity verification.

Option D is incorrect. Resetting all passwords and providing them anew is not a practical or secure approach to collaboration between two organizations.

Question 426. An organization recently experienced a malware infection on one of its workstations. A security analyst has been tasked with reviewing the endpoint logs of the infected system to gather more information about the incident. Which of the following entries in the endpoint logs would be MOST

indicative of the initial malware infection point?

- (A) Logs indicating successful user login and logout events
- (B) Entries showing periodic system health-check status as "OK"
- (C) **Logs documenting a recently installed and executed unknown .exe file from a temporary directory**
- (D) Entries detailing network connectivity checks to the domain controller

Explanation 426. Correct Answer: C. Logs documenting a recently installed and executed unknown .exe file from a temporary directory. Endpoint logs that document the installation and execution of an unknown .exe file, especially from a temporary directory, are strong indicators of potentially malicious activity. Such logs can pinpoint the initial infection point of malware on a system.

Option A is incorrect. User login and logout events are routine logs and do not provide specific information about malware infections unless associated with other suspicious activities.

Option B is incorrect. System health-check status entries are meant to provide general information about the system's health and do not specify actions or changes made on the system related to malware.

Option D is incorrect. Network connectivity checks to domain controllers are routine in many network environments and don't directly indicate malware activity.

Question 427. GammaTech has a new remote access policy for its employees. Whenever an employee attempts to access the corporate network from an unfamiliar location, the system requests additional verification before granting access. Which factor of authentication is being emphasized in this policy?

- (A) Knowledge-based questions the employee answers
- (B) A fingerprint scan from the employee
- (C) **The physical coordinates of the employee's access point**
- (D) An SMS code sent to the employee's phone

Explanation 427. Correct Answer: C. The physical coordinates of the employee's access point. By verifying the location or coordinates of an access point, GammaTech is utilizing the “somewhere you are” factor in multifactor authentication. This emphasizes the geographic location of the user.

Option A is incorrect. Knowledge-based questions fall under the “something you know” factor since users answer based on information they recall.

Option B is incorrect. A fingerprint scan pertains to the “something you are” factor as it’s a biometric, a unique physical characteristic of the individual.

Option D is incorrect. An SMS code sent to a phone belongs to the “something you have” factor, as it’s sent to a device in the user’s possession.

Question 428. AlphaTech’s IT department is rolling out a new authentication protocol for remote workers. As part of the multifactor authentication process, employees are required to provide information that is memorized and cannot be physically taken from them. Which of the following represents this type of authentication factor?

- (A) Fingerprint
- (B) Smart card
- (C) PIN
- (D) USB security key

Explanation 428. Correct Answer: C. PIN. A Personal Identification Number (PIN) represents the “something you know” factor in multifactor authentication. This type of information is memorized by the user and is not a physical item that can be taken or a biological trait.

Option A is incorrect. A fingerprint represents the “something you are” factor, which pertains to biometrics.

Option B is incorrect. A smart card represents the “something you have” factor, as it’s a physical item that a user possesses.

Option D is incorrect. A USB security key also falls under the “something you have” factor. It’s a physical device rather than memorized information.

Question 429. A company has set up its firewall to allow web traffic through port 80 and port 443, while denying all other traffic by default. This setup is an example of which type of access control?

- (A) Role-Based Access Control (RBAC)
- (B) Mandatory Access Control (MAC)
- (C) Discretionary Access Control (DAC)
- (D) **Rule-Based Access Control (RAC)**

Explanation 429. Correct Answer: D. Rule-Based Access Control (RAC). Rule-Based Access Control (RAC) operates based on predefined rules set by administrators. In the scenario described, the firewall is using rules to allow traffic on certain ports (80 and 443) while denying all others, making this a clear example of RAC.

Option A is incorrect. RBAC assigns permissions based on roles within an organization. Firewall rules are not typically assigned based on user roles.

Option B is incorrect. MAC involves classifying information and matching user clearance levels to these classifications. It is unrelated to firewall rule settings.

Option C is incorrect. DAC allows resource owners to specify who can access their resources. Firewall rule settings don't operate based on individual discretion.

Question 430. The security team at WidgetCorp is trying to identify potential insider threats. They have set up a SIEM solution with a custom dashboard showing unusual activities. Which of the following dashboard views would be MOST effective for quickly identifying an employee uploading large amounts of proprietary data to an external cloud storage service?

- (A) Display of users who logged in during off-hours
- (B) **Graph of highest network bandwidth users**
- (C) List of most frequently used applications
- (D) Visualization of failed login attempts

Explanation 430. Correct Answer: B. Graph of highest network bandwidth users. When an employee uploads large amounts of data to an external service, it typically results in a significant spike in network bandwidth. Therefore, a dashboard view that visually displays the highest network bandwidth users can quickly alert the security team to potential data exfiltration activities.

Option A is incorrect. While logging in during off-hours can be suspicious, it doesn't directly correlate to data upload activities.

Option C is incorrect. A list of the most frequently used applications might help in determining the common tools used within the organization, but it doesn't specifically point to data upload actions.

Option D is incorrect. Visualization of failed login attempts could show potential brute-force or unauthorized access attempts, but it doesn't directly indicate data uploading activities.

Question 431. Sarah is a project manager and is working on a document that she owns. She wants to grant specific permissions to certain team members, allowing some to edit and others only to view the document. Which of the following

access control models would BEST allow Sarah to accomplish this?

- (A) Mandatory Access Control (MAC)
- (B) Role-Based Access Control (RBAC)
- (C) **Discretionary Access Control (DAC)**
- (D) Attribute-Based Access Control (ABAC)

Explanation 431. Correct Answer: C. Discretionary Access Control (DAC). DAC allows the owner of the resource (in this case, Sarah) to specify who can access it and what permissions they have (e.g., read, write, execute). This flexibility is what Sarah needs to grant specific permissions to individual team members based on her discretion.

Option A is incorrect. Mandatory Access Control (MAC) is based on classifications and clearance levels. It wouldn't be suitable for Sarah's needs in this scenario.

Option B is incorrect. Role-Based Access Control (RBAC) assigns permissions based on roles in the organization. It wouldn't allow Sarah the fine-grained control she needs over individual permissions.

Option D is incorrect. Attribute-Based Access Control (ABAC) bases access on attributes of the user, environment, and resource itself. While flexible, it's not centered around the owner's discretion in the same way DAC is.

Question 432. CyberSec Corp's CISO wants to determine if there have been any anomalies in user behavior over the past month. Specifically, they're concerned about unauthorized data

transfers outside of regular business hours. Which of the following automated reports would be MOST useful in this investigation?

- (A) After-hours network activity reports
- (B) User password change frequency reports
- (C) Hardware inventory audit reports
- (D) Software licensing compliance reports

Explanation 432. Correct Answer: A. After-hours network activity reports. For the specific concern of unauthorized data transfers outside of regular business hours, the after-hours network activity reports would be most useful. These reports would provide details on network activities, including data transfers, that took place outside typical working hours.

Option B is incorrect. While user password change frequency reports might indicate if users are frequently changing passwords, which could be a sign of suspicious activity, it wouldn't directly address the concern of data transfers outside of regular hours.

Option C is incorrect. Hardware inventory audit reports would provide information about the hardware assets of the company but wouldn't give insights into data transfer activities.

Option D is incorrect. Software licensing compliance reports would detail the compliance status of software licenses, which isn't relevant to the concern about unauthorized data transfers after hours.

Question 433. After detecting suspicious activity on a network, a digital forensic analyst is dispatched to acquire data from a potential compromised system. The analyst decides to capture an image of the affected system's memory. This technique of capturing volatile data is particularly beneficial because:

- (A) It helps identify deleted files
- (B) **It can capture data in real-time operations**
- (C) It provides information on patch levels
- (D) It offers insights into firewall configurations

Explanation 433. Correct Answer: B. It can capture data in real-time operations. Memory acquisition allows forensic analysts to capture data in its current state, including data about running processes, open network connections, and contents of the system's RAM. This can provide insights into malware or unauthorized activities that occurred in real-time.

Option A is incorrect. While memory acquisition can sometimes provide information about recently accessed files, identifying deleted files is typically done through disk imaging and not memory acquisition.

Option C is incorrect. Information about patch levels is usually gleaned from system configurations and logs, not directly from memory acquisition.

Option D is incorrect. Firewall configurations are typically found in system configurations and logs, not directly from a memory acquisition.

Question 434. During a suspected security incident involving unauthorized access to sensitive data, Jake, an IT administrator, immediately disconnected the affected server from the network. Later, a digital forensic expert criticized Jake's action. Which of the following is the MOST likely reason for the criticism?

- (A) Jake should have left the server connected to capture more evidence from the attacker
- (B) Jake should have immediately informed the company's legal department
- (C) **Jake should have taken an image of the server's memory before disconnecting it**
- (D) Jake should have updated the server's software to prevent further unauthorized access

Explanation 434. Correct Answer: C. Jake should have taken an image of the server's memory before disconnecting it. Preserving the current state of a system, especially its volatile memory, is crucial during a digital forensic investigation. Volatile memory can contain critical evidence about an incident, but this evidence is lost once the system is powered off or restarted.

Option A is incorrect. While sometimes monitoring an attacker can be valuable, it's often more critical to prioritize the safety of data and systems over collecting additional evidence.

Option B is incorrect. Although informing the legal department is an important step in many incident response processes, preserving the integrity and state of potential evidence comes first.

Option D is incorrect. While updating the server's software might be a future step to prevent incidents, the immediate priority during a suspected security incident is to preserve evidence.

Question 435. A large enterprise is deploying a new automation system that will allow various teams, including development, operations, and QA, to provision and configure their own environments. The security team is concerned about potential misconfigurations or excessive permissions being granted. Which solution can be used within the automation to ensure security standards are met without limiting the agility of the teams?

- (A) Implementing a zero-trust model for all teams
- (B) Manually reviewing all requests before provisioning
- (C) **Setting up guard rails within the automation scripts to define boundaries and prevent misconfigurations**
- (D) Disabling the automation system for all teams except the security team

Explanation 435. Correct Answer: C. Setting up guard rails within the automation scripts to define boundaries and prevent misconfigurations. Guard rails in automation scripts act as safeguards, ensuring that certain actions, configurations, or provisions stay within defined security and operational boundaries without impeding the benefits of automation.

Option A is incorrect. While a zero-trust model is beneficial for security, it does not directly address the challenge of misconfigurations in automation processes.

Option B is incorrect. Manually reviewing all requests negates the efficiency benefits of automation and slows down the provisioning process.

Option D is incorrect. Disabling the automation system for all teams except the security team defeats the purpose of having an automation system for diverse teams and reduces agility.

Question 436. After a security breach, Jake, a digital forensics investigator, arrives at the scene to collect a hard drive for examination. He labels the hard drive, records its serial number, photographs the scene, and ensures the hard drive is transported securely to the forensics lab. These steps are crucial to:

- (A) Preserve the data's integrity on the hard drive
- (B) **Maintain the chain of custody**
- (C) Decrypt the data on the hard drive
- (D) Implement a legal hold on the data

Explanation 436. Correct Answer: B. Maintain the chain of custody. Maintaining a chain of custody is crucial to ensure that evidence is authentic and unchanged. This involves documenting each step of the evidence handling process, from collection to analysis, ensuring its validity in legal proceedings.

Option A is incorrect. While preserving the data's integrity is crucial in forensics, the specific steps mentioned are primarily for maintaining the chain of custody.

Option C is incorrect. Decrypting the data focuses on making encrypted data readable. The steps Jake took are related to documenting evidence handling, not decryption.

Option D is incorrect. Implementing a legal hold ensures that specific data is preserved for legal reasons. The steps mentioned by Jake focus on documenting how the evidence was handled and preserved, not on a directive to retain it for legal purposes.

Question 437. After deploying a new version of your company's internal application, several users reported issues with accessing specific features. To investigate the root cause, you decided to review the application logs. What entry in the logs would most directly indicate a software bug or error related to the recent deployment?

- (A) Entries showing successful user authentication timestamps
- (B) Entries detailing the number of transactions completed by the application
- (C) **Entries with "ERROR" or "EXCEPTION" related to the specific feature being accessed**
- (D) Entries showing routine data backup operations

Explanation 437. Correct Answer: C. Entries with "ERROR" or "EXCEPTION" related to the specific feature being accessed. In the context of application logs, entries labeled as "ERROR" or "EXCEPTION" generally indicate that the application encountered a problem. If these entries are related to the feature users are having trouble with, it points towards a software bug or issue related to the deployment.

Option A is incorrect. Successful user authentication entries would indicate that users are able to log into the application successfully, but they don't provide insights into feature-specific issues.

Option B is incorrect. While the number of transactions could provide performance metrics or usage patterns, it doesn't directly indicate a software bug or deployment-related issue.

Option D is incorrect. Routine data backup operations are unrelated to application feature functionalities and won't help in identifying deployment-related errors.

Question 438. After a major data breach in XYZ Corporation, the management decided to understand the primary reason behind the incident to prevent such occurrences in the future. Which of the following approaches should the incident response team prioritize to determine the fundamental cause of the breach?

- (A) Perform vulnerability scanning on all servers
- (B) Review firewall logs for the past week
- (C) **Conduct a root cause analysis**
- (D) Upgrade all security software

Explanation 438. Correct Answer: C. Conduct a root cause analysis. Root cause analysis (RCA) is a systematic process for identifying the origin of problems or faults and deciding on the most suitable approach to take to prevent recurrence. In the context of a security incident, RCA helps in determining the primary reason behind the breach.

Option A is incorrect. While vulnerability scanning is essential for understanding potential weaknesses in servers, it does not directly identify the fundamental cause of a past incident.

Option B is incorrect. Firewall logs can provide insights about traffic patterns and potential attacks but may not directly reveal the root cause of a breach.

Option D is incorrect. Upgrading security software is a reactive measure and does not ensure understanding or addressing the core reason for a breach.

Question 439. A cloud infrastructure team frequently receives performance alerts from various resources in the environment. They want to ensure that relevant teams are immediately informed and can act upon any resource that crosses a performance threshold. What is the BEST way to accomplish this?

- (A) Conduct a weekly meeting to review all performance alerts
- (B) Automate ticket creation for any resource that crosses the performance threshold and assign it to the relevant team**
- (C) Send all performance alerts to the cloud infrastructure team's email for review
- (D) Disable performance monitoring to reduce alert fatigue

Explanation 439. Correct Answer: B. Automate ticket creation for any resource that crosses the performance threshold and assign it to the relevant team. Automating the ticket creation process ensures that alerts are not overlooked and that the appropriate teams are informed in real-time, allowing for prompt resolution.

Option A is incorrect. Conducting a weekly review does not allow for immediate action upon critical performance issues.

Option C is incorrect. Sending all alerts to the team's email might lead to alert fatigue and the possibility of overlooking critical alerts among less important ones.

Option D is incorrect. Disabling performance monitoring would prevent the team from receiving important alerts and is not a practical solution.

Question 440. A development team is working on a mission-critical application for a financial institution. The team wants to ensure that any code changes do not introduce vulnerabilities or break existing functionalities. What is the BEST automation approach to achieve this objective?

- (A) Manually review the code changes once a month
- (B) **Use continuous integration tools to automatically compile and test code changes against known vulnerabilities and functional tests**
- (C) Rely on users to report any issues after the application is deployed
- (D) Implement a firewall to block potential attacks on the application

Explanation 440. Correct Answer: B. Use continuous integration tools to automatically compile and test code changes against known vulnerabilities and functional tests.

Continuous integration tools can be set up to automatically test code changes as they are committed. This ensures that

vulnerabilities and functional issues are detected early in the development process.

Option A is incorrect. Manually reviewing code changes once a month does not provide immediate feedback to developers and could delay the identification of vulnerabilities or functional issues.

Option C is incorrect. Relying on users to report issues is reactive and could expose the financial institution to risks if vulnerabilities are exploited.

Option D is incorrect. While firewalls are important for security, they don't address the need to test code changes for vulnerabilities or functional issues.

Question 441. Acme Corp. is in the early stages of a potential lawsuit, and their legal department has just issued a notice for e-discovery related to email communications of a former executive. As an IT security professional, which of the following should be your FIRST action?

- (A) Start a full backup of the company's email server
- (B) **Identify and isolate the email accounts related to the former executive**
- (C) Immediately delete all emails that are more than two years old
- (D) Inform the media about the upcoming lawsuit

Explanation 441. Correct Answer: B. Identify and isolate the email accounts related to the former executive. In the context of e-discovery, it's crucial to locate and preserve

electronically stored information (ESI) that could be relevant to the lawsuit. The first step would be to identify and isolate the specific email accounts or data sources relevant to the request to ensure they are not tampered with or deleted.

Option A is incorrect. While backups are essential, a blanket backup of the email server may not specifically cater to the e-discovery request. Focusing on the particular data in question is more pertinent.

Option C is incorrect. Deleting potential evidence, especially after a notice for e-discovery, could lead to legal penalties and is not a recommended action.

Option D is incorrect. Informing the media is not a primary step in the e-discovery process and can have detrimental effects on the company's reputation.

Question 442. OmegaHealth, a large healthcare provider, is integrating automation into its operations. When a new healthcare worker is hired, they require access to multiple systems. Why would OmegaHealth automate the user provisioning process across these systems?

(A) To enforce a uniform password for all healthcare workers.

(B) To save time by ensuring consistent and simultaneous account creation across all necessary platforms

(C) To prevent the new hires from accessing any system until their probation period ends

(D) To reduce the software licenses needed by delaying account activation

Explanation 442. Correct Answer: B. To save time by ensuring consistent and simultaneous account creation across all necessary platforms. Automating user provisioning, especially in an environment where access to multiple systems is needed, can dramatically save time and reduce human errors. With automation, accounts can be created consistently and simultaneously across all required platforms.

Option A is incorrect. Enforcing a uniform password for all users is a poor security practice. Automation should focus on efficiency and security, not creating potential vulnerabilities.

Option C is incorrect. Automating user provisioning doesn't inherently prevent new hires from accessing systems. The automation should be designed to provision based on specific rules and roles.

Option D is incorrect. Automation in user provisioning is about streamlining the creation and management of accounts, not about reducing software licenses or delaying activations.

Question 443. During a regular review of system logs, Alex, a security analyst, noticed an unusual pattern of network traffic originating from a single IP address. Instead of waiting for an automated system to flag this as suspicious, he decides to manually dive deeper into the data to identify any potential threats. What is Alex engaging in?

(A) Incident management

- (B) Threat modeling
- (C) **Threat hunting**
- (D) Security monitoring

Explanation 443. Correct Answer: C. Threat hunting. Threat hunting is a proactive approach where security professionals or analysts actively and manually search for signs of malicious activities within their network or systems, especially those threats that haven't been automatically detected by traditional security tools.

Option A is incorrect. Incident management refers to the process followed when managing and responding to a security incident. In this scenario, Alex is taking a proactive approach to find potential threats, not responding to an identified incident.

Option B is incorrect. Threat modeling involves identifying potential threats and designing countermeasures to prevent or mitigate the impact of those threats. It's more about planning than actively searching for threats.

Option D is incorrect. Security monitoring is the process of continuously monitoring and analyzing an organization's security events. While Alex is reviewing logs, which is part of monitoring, the manual and proactive deep dive he is taking is more in line with threat hunting.

Question 444 OmegaTech's security team noticed an increase in account compromises. An internal investigation revealed that many employees have been using the same passwords across different company systems and applications. Which password

best practice can OmegaTech enforce to mitigate this issue?

- (A) Encouraging users to change their passwords every month
- (B) Implementing an account lockout policy after three failed login attempts
- (C) **Prohibiting password reuse for at least the last five password changes**
- (D) Mandating that passwords contain only alphabetical characters for simplicity

Explanation 444. Correct Answer: C. Prohibiting password reuse for at least the last five password changes. By prohibiting password reuse for a number of iterations, you discourage users from cycling between a small set of passwords and, therefore, increase the overall security of user accounts.

Option A is incorrect. While frequent password changes can enhance security, they don't directly address the issue of password reuse across different systems and applications.

Option B is incorrect. While an account lockout policy can deter brute-force attacks, it doesn't prevent users from reusing the same passwords across different platforms.

Option D is incorrect. Restricting passwords to only alphabetical characters reduces complexity and weakens the security of the password.

Question 445. AlphaCorp's IT department is reviewing password policies and wants to adopt a strategy that enhances security. Which of the following password strategies would be

the MOST secure?

- (A) Passwords should be at least 6 characters long, with no other requirements
- (B) Passwords should be at least 10 characters long and include both uppercase and lowercase letters
- (C) Passwords should be at least 8 characters long and include uppercase letters, lowercase letters, numbers, and special characters**
- (D) Passwords should be at least 4 characters long and include a mix of uppercase and lowercase letters

Explanation 445. Correct Answer: C. Passwords should be at least 8 characters long and include uppercase letters, lowercase letters, numbers, and special characters. This option provides a balanced combination of length and complexity, making it more resistant to brute-force and dictionary attacks.

Option A is incorrect. A 6-character password without any complexity requirements is easier to crack with modern computational capabilities.

Option B is incorrect. While having a 10-character length is beneficial, it lacks the additional complexity of numbers and special characters which can further bolster security.

Option D is incorrect. The length is too short, and even with a mix of uppercase and lowercase, it does not provide the recommended security for passwords.

Question 446. A security analyst is reviewing the IPS logs and discovers multiple alerts originating from a single IP address attempting to access various company servers. The analyst is trying to determine the type of attack. Which of the following log entries BEST indicates a port scanning activity?

- (A) **Multiple consecutive connection attempts to different ports on a single server in a short time frame**
- (B) Repeated connection attempts to port 80 of a web server every 3 seconds
- (C) Numerous failed login attempts to an FTP server from the same IP address
- (D) Consistent pings to the network gateway every 5 seconds

Explanation 446. Correct Answer: A. Multiple consecutive connection attempts to different ports on a single server in a short time frame. Port scanning is an activity where an attacker probes a server or host to determine what services are running. Rapid connection attempts to various ports indicate that the attacker is trying to discover open ports and the services running on them.

Option B is incorrect. While repeated connection attempts to a single port could be suspicious, it doesn't indicate port scanning. This could be indicative of a DoS attack.

Option C is incorrect. Multiple failed login attempts indicate a possible brute force attack on the FTP server, not port scanning.

Option D is incorrect. Regular pings to the network gateway might be indicative of network mapping or checking connectivity but doesn't suggest port scanning activity.

Question 447. As part of a cloud infrastructure project, AlphaTech plans to deploy multiple virtualized resources for its new application. The deployment includes databases, web servers, and load balancers. What is the PRIMARY benefit of using automation scripts in the resource provisioning process for this project?

- (A) It enables AlphaTech to use a single operating system for all resources
- (B) It guarantees 100% uptime for all virtualized resources
- (C) **It ensures standardized, repeatable, and rapid deployments across the infrastructure**
- (D) It prevents unauthorized users from accessing the cloud infrastructure

Explanation 447. Correct Answer: C. It ensures standardized, repeatable, and rapid deployments across the infrastructure. Automation in resource provisioning provides consistency in deployments, allowing for standardized configurations, rapid scaling, and the ability to repeat deployments without human error.

Option A is incorrect. While automation can deploy similar or consistent environments, it does not inherently enforce a single operating system.

Option B is incorrect. Automation can increase efficiency and reduce human errors, but it cannot guarantee 100% uptime, as

there are other factors involved, like hardware failures or network issues.

Option D is incorrect. While automation can implement security configurations, it does not, by itself, prevent unauthorized access. Security measures need to be designed and implemented separately.

Question 448. DeltaTech, a progressive tech firm, is aiming to improve its security posture by eliminating the vulnerabilities associated with password use. They are considering deploying a passwordless authentication system. Which of the following represents the PRIMARY advantage of such a system?

- (A) It allows users to choose any password complexity
- (B) **It eliminates the need for remembering passwords**
- (C) It guarantees protection against all cyber threats
- (D) It ensures compatibility with all legacy systems

Explanation 448. Correct Answer: B. It eliminates the need for remembering passwords. Passwordless authentication methods, such as biometrics, hardware tokens, or mobile app confirmations, remove the need for users to remember and input passwords. This can reduce risks associated with weak or reused passwords and enhance user convenience.

Option A is incorrect. Passwordless systems remove the concept of a traditional password altogether, so there's no "password complexity" to choose.

Option C is incorrect. While passwordless authentication can significantly enhance security, especially against threats like

password spraying or credential stuffing, it doesn't guarantee protection against all cyber threats.

Option D is incorrect. Passwordless authentication methods might not be compatible with all legacy systems without modifications or updates.

Question 449. OmegaTech recently introduced an additional layer of security for its remote server access. Along with their usual passwords, employees now need to use a physical device they have with them to gain access. Which of the following represents this “something you have” factor in multifactor authentication?

- (A) Password hint
- (B) Facial recognition
- (C) **Hardware token**
- (D) Voice recognition

Explanation 449. Correct Answer: C. Hardware token.

Hardware tokens are devices that generate security codes for authentication purposes. Users are required to have this physical device on-hand, making it an example of the “something you have” factor in multifactor authentication.

Option A is incorrect. A password hint is related to “something you know” factor. Moreover, it's not an authentication factor but rather an aid for recalling a password.

Option B is incorrect. Facial recognition pertains to the “something you are” factor, which refers to biometric methods of authentication.

Option D is incorrect. Voice recognition, similar to facial recognition, falls under the “something you are” factor, as it uses biometric identification.

Question 450. A large corporation is investigating a potential insider threat incident. A security analyst is tasked with examining the OS-specific security logs of a Windows server where sensitive documents are stored. Which of the following entries in the logs would MOST likely indicate unauthorized access attempts?

- (A) Logs displaying Windows Update successful installations
- (B) Entries showing a large number of failed login attempts followed by a successful login from a user outside of regular business hours**
- (C) Logs indicating scheduled disk defragmentation tasks
- (D) Entries detailing successful printer connections and print jobs

Explanation 450. Correct Answer: B. Entries showing a large number of failed login attempts followed by a successful login from a user outside of regular business hours. A sequence of failed login attempts followed by a successful login, especially outside of regular business hours, can be a strong indicator of a brute-force attack or unauthorized access attempt on a system.

Option A is incorrect. Successful installations of Windows Updates are routine maintenance activities and do not directly imply unauthorized access.

Option C is incorrect. Disk defragmentation tasks are part of regular system maintenance and are not indicative of unauthorized access.

Option D is incorrect. While monitoring printer connections and print jobs can be relevant in certain security investigations, they are not direct indicators of unauthorized server access.

Question 451. ThetaTech, a financial institution, wants to upgrade its authentication system for high-net-worth customers accessing their accounts online. Besides the traditional password, they want to include a method that captures unique physical or behavioral characteristics. Which type of authentication method should ThetaTech consider?

- (A) Token-based authentication
- (B) Geolocation tracking
- (C) **Biometrics**
- (D) Smart card

Explanation 451. Correct Answer: C. Biometrics. Biometrics authentication involves recognizing an individual based on their unique physical or behavioral characteristics, such as fingerprints, retina scans, or voice recognition.

Option A is incorrect. Token-based authentication provides users with a device or software token that generates a time-sensitive code. It doesn't capture physical or behavioral characteristics.

Option B is incorrect. Geolocation tracking determines a user's location but doesn't involve capturing unique physical or behavioral traits.

Option D is incorrect. A smart card is a physical card that contains electronic information. It can be used for authentication, but it does not inherently capture unique physical or behavioral characteristics.

Question 452. The cybersecurity team of XYZ Corp. plans to assess their organization's preparedness for a potential data breach. They aim to evaluate the effectiveness of their response strategy without performing any real actions. Which of the following methods would BEST help them achieve this goal?

- (A) Live fire exercise
- (B) System hardening test
- (C) Red team/blue team exercise
- (D) **Tabletop exercise**

Explanation 452. Correct Answer: D. Tabletop exercise. A tabletop exercise is a discussion-based session where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation. It allows for an assessment of an incident response strategy without performing any actual tasks.

Option A is incorrect. A live fire exercise is a real-world test, often unannounced, and could impact actual operations.

Option B is incorrect. System hardening test focuses on making a system more secure against attacks and does not evaluate incident response.

Option C is incorrect. Red team/blue team exercises involve simulating real-world cyber attacks to test an organization's defense and response capabilities, which is more hands-on than what is described.

Question 453. In preparation for a potential lawsuit, Meg, a cybersecurity analyst, has been asked to ensure that specific digital evidence remains intact and is not altered or deleted. What measure should Meg implement to ensure this requirement?

- (A) Encrypt the evidence
- (B) **Initiate a legal hold**
- (C) Perform a full disk wipe
- (D) Conduct a vulnerability assessment

Explanation 453. Correct Answer: B. Initiate a legal hold. A legal hold ensures that specific data that could be relevant to a legal case is preserved and not altered or deleted until the hold is lifted. In this situation, Meg would initiate a legal hold to keep the digital evidence intact for the potential lawsuit.

Option A is incorrect. Encrypting the evidence can ensure its confidentiality, but it does not prevent deletion or guarantee its preservation for legal reasons.

Option C is incorrect. Performing a full disk wipe would eliminate all data on a disk, which is contrary to the requirement of preserving specific digital evidence.

Option D is incorrect. Conducting a vulnerability assessment is about identifying weaknesses in a system, not about preserving digital evidence for legal purposes.

Question 454. A financial company is designing a new system that needs to ensure data is accessed based on classifications and clearance levels of the users. Which of the following access control models BEST fits this requirement?

- (A) Role-Based Access Control (RBAC)
- (B) Discretionary Access Control (DAC)
- (C) **Mandatory Access Control (MAC)**
- (D) Attribute-Based Access Control (ABAC)

Explanation 454. Correct Answer: C. Mandatory Access Control (MAC). MAC is based on the classification of information and the clearance level of users. In a MAC model, the operating system constrains the ability of a subject or initiator to access or perform some sort of operation on an object or target. In this scenario, where data is classified and users are given clearance levels, MAC is the most suitable model.

Option A is incorrect. Role-Based Access Control (RBAC) assigns permissions to specific roles in an organization. Users are then assigned to roles. While useful in many contexts, it doesn't focus on classifications and clearance levels.

Option B is incorrect. Discretionary Access Control (DAC) allows the owner of the resource to specify who can access it. It's more flexible but less restrictive than MAC.

Option D is incorrect. Attribute-Based Access Control (ABAC) uses policies to determine access, based on attributes of users, the environment, and the resource itself. While it can be used in scenarios with classifications and clearances, it's not as strictly based on these factors as MAC.

Question 455. The incident response team at XYZ Corp received a report that an attacker successfully exploited a vulnerable web application in their environment. To identify which server might have been compromised, the team decided to cross-reference recent vulnerability scan results. Which of the following information from the vulnerability scan would be MOST helpful in pinpointing the potentially compromised server?

- (A) The timestamp of when the scan was conducted
- (B) The software version of the scanning tool
- (C) **List of hosts with the specific vulnerability related to the exploit**
- (D) The total number of vulnerabilities identified during the scan

Explanation 455. Correct Answer: C. List of hosts with the specific vulnerability related to the exploit. In the given scenario, to determine which server may have been compromised, the team should focus on those hosts identified in the vulnerability scan as having the specific vulnerability that matches the exploit used by the attacker.

Option A is incorrect. While the timestamp might indicate when the scan was done, it wouldn't provide specifics about which servers had the vulnerability related to the reported exploit.

Option B is incorrect. Knowing the software version of the scanning tool wouldn't assist in identifying the potentially compromised server.

Option D is incorrect. The total number of vulnerabilities identified doesn't help pinpoint a specific server; it only provides a high-level overview of the security posture.

Question 456. Epsilon Inc. recently hired Jenny as a junior network administrator. To ensure security, they give Jenny only the access permissions necessary to complete her specific tasks, such as monitoring network traffic, but not modifying firewall rules. This approach of granting Jenny's permissions aligns with which security principle?

- (A) Mandatory Access Control (MAC)
- (B) Role-Based Access Control (RBAC)
- (C) Time-of-Day Restrictions
- (D) **Least Privilege**

Explanation 456. Correct Answer: D. Least Privilege. The principle of Least Privilege dictates that users should be granted the minimum levels of access – or the least amount of privileges – necessary to complete their job functions. In Jenny's case, she's only granted the permissions necessary for her role, which aligns with this principle.

Option A is incorrect. MAC involves classifying information and matching user clearance levels to these classifications. Jenny's access isn't based on classifications.

Option B is incorrect. RBAC assigns permissions based on roles within an organization. While Jenny's permissions may be aligned with her role, the scenario specifically emphasizes granting the minimal necessary access, which is a characteristic of Least Privilege.

Option C is incorrect. Time-of-Day Restrictions determine access based on the current time and have no direct relation to the principle of Least Privilege.

Question 457. A company is attempting to verify the legitimacy of an email sent from a senior executive to a number of employees. The email requests the recipients to click on a link and enter their credentials for a "system upgrade." The security team wants to ascertain if the email genuinely came from the executive. Which of the following metadata from the email would be MOST beneficial in this investigation?

- (A) The email's subject line
- (B) The email's send time and date
- (C) **The originating IP address in the email headers**
- (D) The size of the email in bytes

Explanation 457. Correct Answer: C. The originating IP address in the email headers. Email headers often contain metadata about the originating IP address of the email. This can help investigators determine if the email was sent from an

expected location or if it originated from an unfamiliar or suspicious IP, indicating a possible phishing attempt.

Option A is incorrect. The subject line of an email is not typically indicative of its authenticity.

Option B is incorrect. While knowing the send time and date may provide some context, it won't necessarily verify the legitimacy of the email sender.

Option D is incorrect. The size of the email in bytes doesn't offer significant value in determining the authenticity of the email's origin.

Question 458. A cloud-based e-commerce company wants to ensure that its inventory system automatically updates the stock levels on its website and third-party sales platforms whenever a sale occurs. What should the company leverage to achieve this real-time synchronization?

- (A) Regularly backup the inventory system and restore it on the website and sales platforms
- (B) Rely on customers to report discrepancies in stock levels
- (C) **Use Application Programming Interfaces (APIs) to integrate the inventory system with the website and third-party platforms**
- (D) Conduct daily stock audits and manually update all platforms

Explanation 458. Correct Answer: C. Use Application Programming Interfaces (APIs) to integrate the inventory system with the website and third-party platforms. Using

APIs ensures real-time data synchronization between systems. Whenever a sale occurs, the inventory system can automatically update stock levels across all platforms.

Option A is incorrect. Backing up and restoring the inventory system is a reactive and inefficient approach. It won't provide real-time stock updates.

Option B is incorrect. Relying on customers to report stock discrepancies is not proactive and could lead to negative customer experiences and potential lost sales.

Option D is incorrect. Manual updates are time-consuming and prone to human error, and they don't support real-time stock level synchronization.

Question 459. After a series of phishing attacks, the IT department of BetaTech Corp noticed that several employees were using easily guessable passwords. The security team decided to recommend the use of password managers to assist employees in creating and remembering strong passwords.

Which of the following is a PRIMARY benefit of using password managers in this context?

(A) Password managers automatically update the operating system

(B) Password managers can generate and store complex passwords

(C) Password managers always prevent phishing attacks

(D) Password managers allow the reuse of strong passwords across multiple platforms

Explanation 459. Correct Answer: B. Password managers can generate and store complex passwords. Password managers can automatically generate complex passwords that meet a variety of criteria (e.g., length, use of special characters, avoidance of easily guessable terms) and store them securely. This helps users maintain strong, unique passwords for every service they use without needing to remember each one.

Option A is incorrect. Password managers are designed for generating, retrieving, and storing complex passwords, not for updating the operating system.

Option C is incorrect. While password managers can help reduce the risk of successful phishing attacks by storing passwords securely and autofilling them on recognized websites, they don't always prevent phishing attacks, especially if a user is deceived into entering credentials on a fake website.

Option D is incorrect. One of the primary benefits of password managers is to ensure that users have unique passwords for each application or service. Reusing passwords, even if strong, across multiple platforms poses a security risk.

Question 460. A company's online retail website faces DDoS attacks that cause significant downtime. Their current setup relies on manual verification of traffic spikes before mitigation efforts are deployed. What change could BEST enhance the company's reaction time to such attacks in the future?

- (A) Educate users to report slow website loading times
- (B) Manually back up the website data every hour
- (C) **Deploy a web application firewall with automated**

DDoS mitigation features

(D) Increase the website's bandwidth to handle traffic spikes

Explanation 460. Correct Answer: C. Deploy a web application firewall with automated DDoS mitigation features. Deploying a web application firewall (WAF) with automated DDoS mitigation can instantly detect and mitigate attack traffic, significantly improving reaction time to attacks compared to waiting for manual verification.

Option A is incorrect. Relying on users to report slow loading times is reactive and does not guarantee a swift response to DDoS attacks.

Option B is incorrect. Backing up website data is important for recovery, but it doesn't prevent or mitigate active DDoS attacks or improve reaction time.

Option D is incorrect. Merely increasing bandwidth might not be sufficient against DDoS attacks. An attacker can still overwhelm the increased capacity, and it doesn't address the need for swift detection and mitigation.

CHAPTER 5

SECURITY PROGRAM

MANAGEMENT AND OVERSIGHT

Questions 461-540

Question 461. RedFlare Solutions, a financial firm, is storing sensitive client data in a database. The Chief Information Security Officer (CISO) insists that the data should be unreadable even if it's intercepted during transmission or if the storage is compromised. Which encryption standard would best serve this requirement?

- (A) Symmetric encryption using a shared key
- (B) Hashing the data with a one-way function
- (C) Encrypting the entire database using transparent data encryption
- (D) Storing the data in a proprietary format

Question 462. GlobalTech, a software development company, is entering into a partnership with WebSolutions, a web hosting provider. They aim to create a standard set of terms governing their ongoing business transactions, including payment terms, delivery protocols, and warranties. Which type of agreement is most suitable for establishing these foundational terms for future transactions?

- (A) Memorandum of understanding (MOU)
- (B) Non-disclosure agreement (NDA)

- (C) Licensing agreement
- (D) Master service agreement (MSA)

Question 463. TechCorp is implementing a new cloud-based solution. The security team has been tasked with analyzing the risks associated with this project. They've decided to categorize the risks based on their potential impact levels: Low, Medium, High, and Critical. Which type of risk analysis is TechCorp's security team employing?

- (A) Quantitative
- (B) Statistical
- (C) Qualitative
- (D) Financial

Question 464. SecureBank is in the process of selecting a vendor for their new online transaction system. The bank is keen on ensuring the selected vendor has robust security measures and a track record of maintaining those measures. As part of the vendor selection process, which of the following steps is the most relevant to the bank's concerns?

- (A) Checking the vendor's sales growth over the last five years
- (B) Conducting due diligence regarding the vendor's security practices
- (C) Comparing the visual appeal of the vendor's user interface to competitors
- (D) Evaluating the vendor's marketing strategies

Question 465. MegaTech Inc. is in the process of outlining a strategy to ensure that after any disaster, critical applications can be restored to a working state within 4 hours. The

organization also wants to make sure that the data loss does not exceed 1 hour. Which of the following policies is most relevant to achieving this objective?

- (A) Data Retention Policy
- (B) Incident Response Policy
- (C) Disaster Recovery Policy
- (D) Password Policy

Question 466. CyberSecure Inc. is evaluating the financial impact of a potential security breach on its main server. The company has estimated that a breach of this server would lead to a direct financial loss of \$500,000 due to data recovery, legal fees, and fines. Which of the following best represents this estimation?

- (A) Annual Rate of Occurrence (ARO)
- (B) Total Cost of Ownership (TCO)
- (C) Single Loss Expectancy (SLE)
- (D) Annualized Loss Expectancy (ALE)

Question 467. SecureWeb LLC, a web hosting company, has experienced two server breaches over the past five years. They are currently analyzing the risks associated with their infrastructure. Which of the following best represents the Annualized Rate of Occurrence (ARO) for the server breaches?

- (A) 0.2
- (B) 0.4
- (C) 2
- (D) 5

Question 468. An e-commerce company recently faced a DDoS attack that rendered its website unavailable for several hours.

While reflecting on the incident, the CISO emphasized the importance of having a detailed plan that includes identification, containment, eradication, recovery, and lessons learned. Which policy primarily encompasses these stages for handling security incidents?

- (A) Change Management Policy
- (B) Incident Response Policy
- (C) Disaster Recovery Policy
- (D) Remote Access Policy

Question 469. AlphaCorp is in the final stages of selecting a cybersecurity consultant. One of the shortlisted firms, SecureWorld, recently hired AlphaCorp's former CISO as a senior consultant. Given this situation, what should be AlphaCorp's immediate concern during vendor selection?

- (A) The expertise the former CISO brings to SecureWorld
- (B) The possibility that SecureWorld could offer a discounted price
- (C) Potential conflict of interest due to prior associations
- (D) SecureWorld's global presence and reputation

Question 470. WebServ Corp., a web hosting company, has been analyzing the reliability of its servers. They found that one of their server models, on average, tends to fail once every 2000 hours and then gets promptly repaired. Which of the following metrics is WebServ Corp. evaluating?

- (A) Recovery Time Objective (RTO)
- (B) Mean Time To Repair (MTTR)
- (C) Mean Time Between Failures (MTBF)
- (D) Recovery Point Objective (RPO)

Question 471. TechFusion Inc. is a well-established technology company that has been in the market for over 15 years.

Recently, the board of directors decided that the company will pursue aggressive growth strategies by entering new, untested markets and launching cutting-edge products, even if these strategies come with significant risks. How would you classify TechFusion Inc.'s risk appetite?

- (A) Conservative
- (B) Expansionary
- (C) Neutral
- (D) Risk-averse

Question 472. After a significant merger between two large corporations, a comprehensive risk assessment was conducted to identify potential security gaps within the combined infrastructure. This assessment was exclusive to the merger and was not planned to be repeated in the future. What type of risk assessment was this?

- (A) Recurring
- (B) Continuous
- (C) One-time
- (D) Dynamic

Question 473. AcmeTech, a software development firm, recently experienced a major data breach that was traced back to a vulnerability in their custom-built application. Post-incident analysis revealed that the vulnerability had been introduced during the coding phase and was never detected during testing. To avoid such vulnerabilities in the future, which policy should AcmeTech emphasize to ensure secure practices are maintained throughout the development process?

- (A) Incident Response Policy
- (B) Change Management Policy
- (C) Business Continuity Policy
- (D) Software Development Lifecycle (SDLC) Policy

Question 474. An organization is conducting a risk assessment for its cloud infrastructure. The assessment has determined that the likelihood of a data breach through an insecure API is “High.” What factors may have contributed to this likelihood rating?

- (A) The API has been thoroughly tested and has a known secure configuration
- (B) There are few records of this kind of breach in the industry
- (C) The API is publicly accessible and has had several vulnerabilities reported in the past six months
- (D) The cloud provider offers a guaranteed SLA against any form of security breach

Question 475. SecureNet Ltd. wants to protect user accounts from brute force attacks. They want to implement a measure where, after a certain number of failed login attempts, the account would become temporarily inaccessible. Which standard best suits this requirement?

- (A) Password minimum length
- (B) Account lockout threshold
- (C) Mandatory password resets
- (D) Two-factor authentication

Question 476. After a recent security breach, CyberSolutions Inc. evaluated their response metrics and determined that, on

average, it took 4 hours from identifying a security breach to having it completely resolved. Which metric best describes this 4-hour timeframe?

- (A) Recovery Time Objective (RTO)
- (B) Recovery Point Objective (RPO)
- (C) Mean Time Between Failures (MTBF)
- (D) Mean Time To Repair (MTTR)

Question 477. SecureCom, a telecommunications company, is planning to expand its infrastructure across Country A. The nation recently updated its telecommunications regulations and mandates strict guidelines for all external communications. Which of the following should be SecureCom's primary focus as it begins its expansion?

- (A) Increasing advertising budget to gain a stronger market presence in Country A
- (B) Ensuring its infrastructure meets the national standards for secure and encrypted communications
- (C) Collaborating with local tech companies to better understand the culture of Country A
- (D) Launching new products tailored to the preferences of Country A's residents

Question 478. During an audit review at NetSecure Corp., the external auditors observed that the company is willing to take risks that can potentially result in a 10% decrease in their annual profits, but no more than that. The auditors want to document this finding in their report. Which term should they use to describe NetSecure Corp.'s stance?

- (A) Risk Avoidance
- (B) Risk Transfer

- (C) Risk Tolerance
- (D) Risk Assessment

Question 479. TechGuard Corp. conducts a risk assessment every six months to identify new vulnerabilities and ensure that previous risk-mitigation strategies remain effective. This type of risk assessment is best described as:

- (A) Periodic
- (B) Ad hoc
- (C) Continuous
- (D) Recurring

Question 480. CyberFleet Inc., a software development company, has just heard of a newly discovered vulnerability in a third-party library they heavily rely upon. The security team quickly gathers to understand and analyze the potential risks associated with this vulnerability. This spontaneous assessment is best described as:

- (A) Routine
- (B) Ad hoc
- (C) Scheduled
- (D) Benchmark

Question 481. TechFlow Corp. is undergoing a risk analysis for its online platform. If a critical vulnerability were exploited, the company would have to pay \$10,000 in repair costs, \$5,000 in compensation to customers, and a \$15,000 fine to regulatory bodies. What would be the Single Loss Expectancy (SLE) for this vulnerability?

- (A) \$10,000
- (B) \$20,000

- (C) \$30,000
- (D) \$50,000

Question 482. GlobalTech, a multinational corporation, is negotiating a cloud storage contract with CloudCorp. GlobalTech wants to ensure that data retrieval times remain under 2 seconds 99.9% of the time. Which component should be explicitly defined in their agreement to set this expectation?

- (A) Pricing model
- (B) Data sovereignty clauses
- (C) Service-level agreement (SLA)
- (D) Termination clauses

Question 483. A software development company is evaluating the risks associated with a newly discovered vulnerability in its application. After reviewing logs and simulating potential attacks, the security team estimates that there is a 0.25 probability of the vulnerability being exploited in the next year. What does this probability indicate?

- (A) The vulnerability has a 1 in 4 chance of being exploited in the next year
- (B) The vulnerability will certainly be exploited four times in the next year
- (C) The vulnerability has been exploited 25 times in the past year
- (D) Every fourth customer will exploit the vulnerability.

Question 484. A global e-commerce company maintains a risk register to keep track of identified risks and to monitor specific metrics that might indicate an increased risk level. Recently, there has been a 20% increase in abandoned shopping carts on

their platform. How should this metric be categorized in the context of the risk register?

- (A) Risk Appetite
- (B) Risk Mitigation Strategy
- (C) Key Risk Indicator (KRI)
- (D) Risk Tolerance Threshold

Question 485. A financial institution has reported that they experience an average of 3 phishing attacks every year that attempt to compromise their user data. Based on this data, what is the Annualized Rate of Occurrence (ARO) for these phishing attacks?

- (A) 0.33
- (B) 1
- (C) 3
- (D) 12

Question 486. During a board meeting at DataFlow Corp., the CEO emphasizes that while they are willing to take certain risks for innovation, there's a limit to the amount of risk they are willing to take, especially concerning potential financial losses. To ensure that risks stay below this level, what should be defined in the risk register?

- (A) Risk Owner Assignment
- (B) Key Risk Indicator (KRI)
- (C) Risk Impact Analysis
- (D) Risk Threshold

Question 487. XYZ Corporation recently implemented a security solution that constantly evaluates the company's threat landscape, monitoring for emerging risks and immediately

alerting the security team of any changes. This assessment model allows the team to rapidly adapt their security posture in response to live threats. What type of risk assessment is XYZ Corporation utilizing?

- (A) One-time
- (B) Periodic
- (C) Dynamic
- (D) Continuous

Question 488. Your organization is considering a partnership with TechVendor Inc., a software solution provider. Before finalizing the agreement, you wish to ensure their application's security. What would be the most direct method to assess the robustness of their system against potential cyber threats?

- (A) Conducting an internal security awareness training
- (B) Reviewing their past audit reports
- (C) Implementing strict firewall rules
- (D) Performing a penetration test on their application.

Question 489. MedGuard, a health tech company, has developed an AI-driven software that predicts potential health risks based on patient data. Before launching in the U.S. market, which of the following industry external considerations should be the company's primary focus?

- (A) Integrating with popular fitness tracking apps in the U.S.
- (B) Ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA)
- (C) Surveying U.S. doctors about software interface preferences

(D) Collaborating with U.S. pharmaceutical companies for promotional deals

Question 490. During a company's onboarding process, new employees are required to read and acknowledge understanding of various company policies. The HR department wants to ensure that employees are aware of their responsibilities when it comes to the use of company devices and internet resources. Which policy should be included in the onboarding packet to address this?

- (A)** Password Complexity Policy
- (B)** Data Classification Policy
- (C)** Acceptable Use Policy (AUP)
- (D)** Vendor Management Policy

Question 491. XYZ Corp is in the process of defining clear roles and responsibilities for their IT assets. During a meeting, the team discussed the primary individual who will have the responsibility for the data within a specific IT system and also be the main point of contact for any decisions related to it. Which of the following roles best describes this individual?

- (A)** System administrator
- (B)** Data custodian
- (C)** System owner
- (D)** End-user

Question 492. As the Chief Security Officer (CSO) of AlphaTech, you are in the process of finalizing a partnership agreement with a third-party provider. To ensure ongoing security compliance and transparency, you want to reserve the right for your organization to inspect the vendor's operations

and security measures in the future. Which clause should you ensure is included in the contract?

- (A) Non-disclosure agreement (NDA)
- (B) Service level agreement (SLA)
- (C) Termination clause
- (D) Right-to-audit clause

Question 493. CyberGuard LLC, a cybersecurity firm, is in a stable position in its industry with consistent returns. The leadership decides not to pursue aggressive growth strategies but instead chooses to maintain its current market share and operational scale. They are open to minor risks but avoid major disruptions. How can one best describe CyberGuard LLC's risk appetite?

- (A) Expansionary
- (B) Neutral
- (C) Conservative
- (D) Aggressive

Question 494. Two university research departments, UniAlpha and UniBeta, decide to collaborate on a project exploring quantum computing's security implications. They need an agreement to express mutual intentions without enforcing legally binding obligations. Which document is most suitable for their needs?

- (A) Service-level agreement (SLA)
- (B) Non-disclosure agreement (NDA)
- (C) Memorandum of understanding (MOU)
- (D) Licensing agreement

Question 495. TechFirm is preparing to embark on a new project with a client, focusing on implementing a cybersecurity infrastructure overhaul. They wish to lay out the specific tasks, deliverables, timelines, and resources required for this project. Which type of agreement would best capture these details?

- (A) Memorandum of understanding (MOU)
- (B) Joint venture agreement
- (C) Master service agreement (MSA)
- (D) Work order (WO)/statement of work (SOW)

Question 496. AcmeBank recently performed a business impact analysis for its online banking system. The result indicated that the bank could tolerate a maximum downtime of 4 hours for the system before incurring significant financial losses and customer dissatisfaction. Which concept best describes this 4-hour period?

- (A) Recovery Point Objective (RPO)
- (B) Maximum Tolerable Downtime (MTD)
- (C) Recovery Time Objective (RTO)
- (D) Time To Restore (TTR)

Question 497. DigitalZone Corp, a marketing company, collects personal data from users and determines how and why that data will be processed. At the same time, they engage an external company, CloudSolutions, to store and manage this data. In this scenario, what role does DigitalZone Corp play in relation to data protection regulations?

- (A) Processor
- (B) Data subject
- (C) Controller
- (D) Third-party provider

Question 498. TechFirm Inc. has decided to engage in a new business venture. Before they move forward, the security team conducts several brainstorming sessions, interviews, and reviews historical data to generate a list of potential security threats that the new venture could face. This activity is a primary component of which step in the risk management process?

- (A) Risk assessment
- (B) Risk response
- (C) Risk monitoring
- (D) Risk identification

Question 499. A healthcare organization uses a software platform to manage patient records. A recent vulnerability assessment identified a potential exploit where an unauthorized individual might gain access to 30% of stored patient data. Which of the following BEST describes this scenario?

- (A) The threat likelihood is 30%
- (B) The vulnerability has a 30% rate of occurrence
- (C) The exposure factor of the vulnerability is 30%
- (D) 30% of the patients have been impacted

Question 500. XYZ Corporation recently faced a major power outage that affected their primary data center. During the incident, it was found that there was no clear guidance on the steps to maintain or quickly restore business operations. To address this, which of the following policies should XYZ Corporation prioritize implementing?

- (A) Data Classification Policy
- (B) Business Continuity Policy

- (C) Acceptable Use Policy
- (D) Network Segmentation Strategy

Question 501. AlphaTech wants to ensure that its remote employees follow best security practices when working from home. The security team has been tasked with drafting a set of guidelines for remote work. What should be the primary focus of these guidelines?

- (A) Outlining punitive measures for non-compliance
- (B) Stating the company's legal position on remote work
- (C) Recommending security measures for home networks and devices
- (D) Dictating the exact software and hardware specifications for remote workers

Question 502. Lisa, a security manager, is reviewing the company's existing policies and realizes that there isn't a comprehensive document detailing the organization's stance, expectations, and commitment to protecting its information assets. Which of the following should Lisa prioritize creating to address this gap?

- (A) Incident Response Plan
- (B) Information Security Policy
- (C) Acceptable Use Policy
- (D) Data Backup Strategy

Question 503. TechFusion and CodeRush, two independent software development companies, are collaborating on a project that is expected to define industry standards for a new coding language. While both parties have an understanding of shared responsibilities, they have not yet established legally binding

obligations. Which type of agreement best suits their current collaborative understanding?

- (A) Service-level agreement (SLA)
- (B) Non-disclosure agreement (NDA)
- (C) Memorandum of agreement (MOA)
- (D) Licensing agreement

Question 504. As part of improving their security posture, TechHive Inc. decided to review their existing password policies. The current policy requires employees to use at least one uppercase letter, one number, and one special character. However, they found that users mostly only make minimal changes to their passwords during resets. Which standard should be integrated into their policy to ensure passwords are more complex and unique over time?

- (A) Password history retention
- (B) Password expiration period
- (C) Account lockout duration
- (D) Maximum password age

Question 505. CyberTech Inc., a cybersecurity consulting company, is in discussions with a potential client, MedCorp, to assist in developing a new secure medical records system. MedCorp will be sharing sensitive patient data with CyberTech as part of the process. Which agreement should be in place before the sharing of such information to ensure confidentiality?

- (A) Memorandum of understanding (MOU)
- (B) Service-level agreement (SLA)
- (C) Non-disclosure agreement (NDA)
- (D) Work order (WO)/statement of work (SOW)

Question 506. AlphaTech is conducting a risk analysis on their new online payment gateway. They've calculated the Annual Rate of Occurrence (ARO) for a specific vulnerability as 2, and the Single Loss Expectancy (SLE) as \$50,000. How much should AlphaTech anticipate losing annually due to this vulnerability?

- (A) \$10,000
- (B) \$100,000
- (C) \$25,000
- (D) \$1,000,000

Question 507. WhiteCape Healthcare, an international healthcare provider, has a large patient database that includes many EU citizens. They're about to implement a new system to improve data access for physicians. Which of the following regulatory requirements should they pay particular attention to when granting physicians access to EU patient data?

- (A) Ensure data is only accessed for tax reporting purposes
- (B) Acquire explicit consent from patients before sharing data
- (C) Encrypt all data using a proprietary algorithm
- (D) Store data in a physical server located within the EU

Question 508. WebFlix, a popular online movie streaming service, experienced a data center outage due to a natural disaster. They had backups in place and restored their systems using data from 6 hours prior to the outage. This resulted in the loss of some user interactions, like ratings and watchlists from the last 6 hours. What term describes the 6-hour gap between the last backup and the time of the outage?

- (A) Recovery Time Objective (RTO)

- (B) Maximum Tolerable Downtime (MTD)
- (C) Recovery Duration Period (RDP)
- (D) Recovery Point Objective (RPO)

Question 509. As a security consultant, you are hired by a multinational corporation to assess the security posture of their potential vendors. One of the vendors appears promising, but your client wants to ensure that the vendor periodically examines and strengthens its own internal procedures and security controls. What should you advise your client to request from this vendor?

- (A) The vendor's business continuity plan
- (B) A list of the vendor's clients
- (C) Evidence of internal audits
- (D) The vendor's company mission statement

Question 510. GlobalFin, a fintech company, has developed a new mobile banking application. To avoid any legal complications, which of the following legal external considerations should GlobalFin pay the most attention to before launching the application worldwide?

- (A) Ensuring the app meets global data privacy laws
- (B) Confirming the color scheme aligns with branding regulations in all countries
- (C) Securing copyrights for all images used in the app
- (D) Making sure the app's name isn't offensive in any language

Question 511. MedTech, a medical device manufacturer, did not adhere to the required standards for device security and patient data protection. Which of the following repercussions

might be the MOST critical for MedTech's ongoing operations?

- (A) Increased public relations campaigns
- (B) Short-term stock price fluctuations
- (C) Offering discounts on their devices
- (D) Loss of license to manufacture and distribute

Question 512. Your organization has been repeatedly ignoring the security guidelines set forth by a global standards organization, despite having pledged adherence. Given the repetitive nature of these violations, the organization is now facing disciplinary measures. Which of the following is the MOST likely immediate consequence of these actions?

- (A) Immediate revocation of business licenses
- (B) Sanctions imposed by the global standards organization
- (C) Forcible shutdown of all online operations for a determined period
- (D) Mandatory public apology to stakeholders

Question 513. HealthCareNow, a large hospital chain, wants to ensure its newly implemented electronic health record (EHR) system adheres to national standards. Which type of audit would be most appropriate to confirm that HealthCareNow is in compliance with national regulations regarding patient data?

- (A) Self-assessment using internal standards
- (B) Third-party risk assessment
- (C) External regulatory audit
- (D) Informal peer review

Question 514. In preparation for an upcoming audit, AlphaTech Corporation hires a team to evaluate their security measures. The team is spotted attempting to bypass security barriers,

unlock doors without keys, and trying to access restricted floors by pretending to be maintenance staff. What type of testing is AlphaTech Corporation undergoing?

- (A) Network vulnerability scanning
- (B) Physical penetration testing
- (C) OS fingerprinting
- (D) Source code review

Question 515. Emily, a cybersecurity analyst, has been tasked with gathering preliminary information about a target organization without directly interacting with its systems. She decides to collect data from third-party sources, search engines, public records, and other online platforms without sending any packets to the target. Which phase of penetration testing is Emily currently engaged in?

- (A) Active reconnaissance
- (B) Passive reconnaissance
- (C) Vulnerability scanning
- (D) Threat hunting

Question 516. As part of an initial penetration testing phase, Jackson is using tools that directly probe and interact with the target system's network to discover open ports, services, and other potential access points. While this approach is more direct and could be detected by the target's security systems, it provides detailed and actionable insights. Which type of reconnaissance is Jackson performing?

- (A) Threat analysis
- (B) Passive reconnaissance
- (C) Active reconnaissance
- (D) Social engineering

Question 517. TechFirm, a leading technology conglomerate, recently conducted a security exercise. The goal was for the internal security team to defend against a series of simulated attacks from an external red team. While the red team launched attacks, the internal team's objective was to detect, respond, and mitigate those threats. What type of penetration testing is TechFirm employing for its internal security team?

- (A) Offensive penetration testing
- (B) Passive penetration testing
- (C) Defensive penetration testing
- (D) Black box testing

Question 518. Emily, an executive assistant, receives a phone call from an individual claiming to be a new employee in the IT department. The caller says they're conducting a routine check and needs Emily to confirm her username and password for system verification. How should Emily respond?

- (A) Politely decline and report the call to the IT department
- (B) Provide the caller with the username but not the password
- (C) Ask the caller to email the request, so there's a written record
- (D) Hang up without saying anything

Question 519. XYZ Corp, a manufacturer of smart home devices, failed to implement standard security practices in their products. A popular tech review site publishes an in-depth review detailing these vulnerabilities. Which of the following outcomes is XYZ Corp MOST likely to face as an immediate result?

- (A) An award for innovation in smart home technologies

- (B) Reputational damage leading to decreased sales
- (C) An increased partnership with tech retailers
- (D) A surge in the employee recruitment rate

Question 520. SoftTech Inc., a software company, is considering expanding its operations to Europe. They will be collecting and processing personal data of EU citizens. Which of the following legal implications is MOST critical for SoftTech Inc. to consider?

- (A) The need to register with each country's software association
- (B) Compliance with the General Data Protection Regulation (GDPR)
- (C) Ensuring software patent rights in each European country
- (D) The European standard for software coding

Question 521. DataGuard Corp. operates in the European Union and has recently suffered a major data breach affecting the personal data of thousands of users. They failed to comply with some key provisions of the General Data Protection Regulation (GDPR). Which of the following is the MOST likely immediate consequence of their non-compliance?

- (A) They will be forced to shut down operations until compliance is achieved
- (B) DataGuard's executive team will face immediate imprisonment
- (C) The company will be required to issue a public apology
- (D) DataGuard Corp. will face substantial fines for their non-compliance

Question 522. SafeNet, a financial institution, decided to undertake a comprehensive security assessment. They brought together their internal security team and an external group of ethical hackers. Their objective was for these teams to collaboratively assess vulnerabilities, perform real-time attack simulations, and evaluate defense mechanisms. What form of penetration testing is SafeNet utilizing?

- (A) Black box testing
- (B) Integrated penetration testing
- (C) Defensive penetration testing
- (D) Red team assessment

Question 523. AlphaTech, a leading tech manufacturer, is considering a penetration test to identify vulnerabilities in their new product's firmware. They provide the testers with firmware source code, architecture diagrams, and other internal details to ensure a thorough evaluation. What kind of penetration test is AlphaTech commissioning?

- (A) Zero-knowledge testing
- (B) Open box testing
- (C) Opaque testing
- (D) Blind testing

Question 524. John, a citizen of a country that strictly follows the General Data Protection Regulation (GDPR), used a global online shopping platform for a year. He decided to stop using the platform and requested the deletion of all his personal data. What is the online platform's primary obligation concerning John's request under the "Right to be Forgotten" principle?

- (A) Retain the data but ensure that John's data is never used for marketing purposes

- (B) Delete all personal data about John unless there's a legal reason to keep it
- (C) Anonymize John's data and notify him of the completion
- (D) Move John's data to a secure, encrypted server where it won't be accessed

Question 525. WebMasters LLC, a popular web hosting company, wants to ensure the robust security of their hosted websites. They initiate a security challenge, inviting ethical hackers worldwide to find vulnerabilities without giving any details about their servers, databases, or applications. Which penetration testing method is WebMasters LLC utilizing?

- (A) External testing
- (B) Grey box testing
- (C) Active testing
- (D) Black box testing

Question 526. After a series of high-profile data breaches in the industry, OnlineRetail Corp., an e-commerce platform, wishes to undergo an external review to validate the security of its operations and provide a comprehensive report to its shareholders. Which type of assessment will provide a detailed and formalized examination of their security posture?

- (A) External examination of IT controls and operations
- (B) Internal review of security protocols
- (C) External regulatory audit on financial statements
- (D) Informal feedback from industry peers

Question 527. WebFirm, a web development company, did not comply with the data handling and protection clauses outlined

in their contract with RetailMax, an e-commerce company. As a result, RetailMax's customer data was exposed in a data breach. Which of the following is the MOST probable contractual impact on WebFirm due to this incident?

- (A) WebFirm will receive bonuses for early project completion
- (B) WebFirm will be required to provide additional services at no cost
- (C) RetailMax will terminate the contract and may seek damages
- (D) RetailMax will extend the project timeline

Question 528. SafeNet Banking Corporation is keen on gaining a competitive edge in the market by demonstrating its commitment to cybersecurity. They want an official attestation that their cybersecurity measures are robust and compliant with industry standards. What should SafeNet opt for to obtain this attestation?

- (A) Feedback from customers on the bank's app security
- (B) Internal IT team's report on cybersecurity practices
- (C) External independent third-party audit
- (D) Informal evaluation by a cybersecurity consultancy

Question 529. XYZ Corp., a multinational company, recently underwent a security audit. The Chief Information Security Officer (CISO) needs to report the findings of the audit to the company's internal stakeholders as well as to a governmental regulatory agency. Which of the following represents the correct type of compliance reporting for each recipient?

- (A) Internal report for the regulatory agency and external report for internal stakeholders

- (B) External report for both the regulatory agency and internal stakeholders
- (C) Internal report for internal stakeholders and external report for the regulatory agency
- (D) No report is required for internal stakeholders, only an external report for the regulatory agency

Question 530. SoftTech Solutions is a software development company that has decided to conduct a penetration test on their new web application. The testers are provided with user credentials, network topology diagrams, and some proprietary software code snippets. Which type of penetration testing is SoftTech Solutions employing?

- (A) Black box testing
- (B) Double-blind testing
- (C) Known environment testing
- (D) Zero-knowledge testing

Question 531. A medium-sized organization recently had a third-party auditor review their information security controls. After the review, the auditor provided a formal statement that verified the effectiveness of the controls in place. What is this formal statement referred to as?

- (A) Certification
- (B) Accreditation
- (C) Attestation
- (D) Assurance

Question 532. CyberLock Inc. is assessing the security postures of its third-party vendors to determine potential risks. The cybersecurity team wants to gather foundational security

information from each vendor to evaluate their security maturity and practices. What would be the most cost-effective and efficient way to collect this data from a large number of vendors?

- (A) Conduct a penetration test for each vendor
- (B) Send out security questionnaires to each vendor
- (C) Visit each vendor's site for an in-person assessment
- (D) Review the annual financial reports of each vendor

Question 533. TechGuard Inc. and CloudSecure are two cybersecurity firms that are considering a collaboration on a new cloud security project. Both companies have proprietary technologies and methodologies they will bring into the partnership. Before embarking on the collaborative venture, which agreement should they finalize to define the terms of their partnership, roles, and shared responsibilities?

- (A) Non-disclosure agreement (NDA)
- (B) Service-level agreement (SLA)
- (C) Business partners agreement (BPA)
- (D) Memorandum of understanding (MOU)

Question 534. XYZ Ltd. wants to evaluate if their current security measures are consistent with industry-specific regulations they are required to follow. The evaluation should be done by their own IT department before inviting external auditors. Which approach should XYZ Ltd. adopt?

- (A) Third-party vulnerability scanning
- (B) Internal compliance assessment
- (C) External attestation
- (D) Vendor risk assessment

Question 535. A cybersecurity firm has been hired by TechGiant Corp. to perform penetration testing on their infrastructure. Before the testing begins, the CEO of TechGiant Corp. wants to ensure that certain critical systems are not targeted, and that the testing will not disrupt their ongoing operations. What should be established to define the scope and boundaries of the test?

- (A) Service-level agreement (SLA)
- (B) Non-disclosure agreement (NDA)
- (C) Rules of engagement (ROE)
- (D) Memorandum of understanding (MOU)

Question 536. As part of the annual security training, the IT department of XYZ Corp decides to launch a simulated phishing campaign. The aim is to assess employees' ability to identify and report phishing emails. Which of the following would be the MOST effective first step in ensuring the success of this campaign?

- (A) Informing all employees about the campaign a week prior
- (B) Creating a realistic phishing email that closely resembles common threats
- (C) Offering rewards to employees who click on the simulated phishing links
- (D) Reviewing the results of the previous year's campaign

Question 537. A healthcare provider wants to evaluate the security of their patient portal. They inform the penetration testers about the technologies used, such as the programming languages and databases. However, specifics about the security measures in place, including intrusion detection systems, are

kept secret. What kind of penetration test are they aiming for?

- (A) White box testing
- (B) External testing
- (C) Grey box testing
- (D) Active testing

Question 538. TechFirm Inc. collects personal data from its users and decides on the purposes and means of processing this data. They also outsource data storage to CloudData, a third-party company. In the context of data privacy regulations, how would TechFirm and CloudData be classified respectively?

- (A) TechFirm: Processor; CloudData: Controller
- (B) TechFirm: Controller; CloudData: Processor
- (C) Both TechFirm and CloudData: Processors
- (D) Both TechFirm and CloudData: Controllers

Question 539. Sarah, a sales manager at TechWorld Inc., receives an email from her bank urging her to update her account details due to a recent security breach. The email provides a link to a website that looks almost identical to her bank's official site. However, she notices a slight misspelling in the URL. What should Sarah do next?

- (A) Forward the email to her colleagues as a warning
- (B) Click the link and update her details as the bank's site is probably just undergoing updates
- (C) Delete the email without taking any action
- (D) Report the email to her company's IT department and avoid clicking any links

Question 540. WebSoft Inc., a leading software company, recently launched a new web application. Before making it live,

they engaged a security firm to challenge the application, find vulnerabilities, and exploit them as real hackers would. This aggressive testing is done to ensure maximum security. What kind of penetration testing is WebSoft Inc. opting for?

- (A) White box testing
- (B) Defensive penetration testing
- (C) Offensive penetration testing
- (D) Gray box testing

Answers 461-540

Question 461. RedFlare Solutions, a financial firm, is storing sensitive client data in a database. The Chief Information Security Officer (CISO) insists that the data should be unreadable even if it's intercepted during transmission or if the storage is compromised. Which encryption standard would best serve this requirement?

- (A) Symmetric encryption using a shared key
- (B) Hashing the data with a one-way function
- (C) **Encrypting the entire database using transparent data encryption**
- (D) Storing the data in a proprietary format

Explanation 461. Correct Answer: C. Encrypting the entire database using transparent data encryption. Transparent data encryption (TDE) encrypts the entire database, ensuring that data remains encrypted both at rest and during transmission. It

renders the data unreadable without the appropriate encryption keys.

Option A is incorrect. Symmetric encryption can make data unreadable, but it may pose challenges in key management and distribution, especially if the key is compromised.

Option B is incorrect. Hashing data makes it unreadable, but it's a one-way function. Once data is hashed, it cannot be retrieved or decrypted, making it unsuitable for encrypting stored data that needs to be accessed and read.

Option D is incorrect. Simply storing data in a proprietary format doesn't mean it's encrypted or unreadable. If someone understands or reverse engineers the format, the data can be read.

Question 462. GlobalTech, a software development company, is entering into a partnership with WebSolutions, a web hosting provider. They aim to create a standard set of terms governing their ongoing business transactions, including payment terms, delivery protocols, and warranties. Which type of agreement is most suitable for establishing these foundational terms for future transactions?

- (A) Memorandum of understanding (MOU)
- (B) Non-disclosure agreement (NDA)
- (C) Licensing agreement
- (D) **Master service agreement (MSA)**

Explanation 462. Correct Answer: D. Master service agreement (MSA). A Master service agreement (MSA) is

designed to define a broad framework covering the terms and conditions of business transactions between parties. It sets out general terms so that specific details can be negotiated in subsequent contracts. Given that GlobalTech and WebSolutions intend to outline foundational terms for their ongoing transactions, an MSA is the most fitting choice.

Option A is incorrect. An MOU establishes mutual intentions but typically doesn't detail specific transaction terms.

Option B is incorrect. An NDA focuses on maintaining confidentiality and doesn't establish transactional terms.

Option C is incorrect. A licensing agreement concerns the rights to use, distribute, or reproduce specific software or intellectual property.

Question 463. TechCorp is implementing a new cloud-based solution. The security team has been tasked with analyzing the risks associated with this project. They've decided to categorize the risks based on their potential impact levels: Low, Medium, High, and Critical. Which type of risk analysis is TechCorp's security team employing?

- (A) Quantitative
- (B) Statistical
- (C) **Qualitative**
- (D) Financial

Explanation 463. Correct Answer: C. Qualitative. Qualitative risk analysis involves assessing risks based on descriptive

categories or rankings, such as Low, Medium, High, and Critical, instead of using numeric values.

Option A is incorrect. Quantitative risk analysis involves using numerical values, often in the form of monetary figures or percentages, to evaluate risks.

Option B is incorrect. Statistical risk analysis uses statistical methods, often paired with quantitative data, to predict future risks. It doesn't categorize risks in the manner described.

Option D is incorrect. Financial risk analysis specifically evaluates risks in terms of potential financial losses and is a subset of quantitative risk analysis.

Question 464. SecureBank is in the process of selecting a vendor for their new online transaction system. The bank is keen on ensuring the selected vendor has robust security measures and a track record of maintaining those measures. As part of the vendor selection process, which of the following steps is the most relevant to the bank's concerns?

- (A) Checking the vendor's sales growth over the last five years
- (B) Conducting due diligence regarding the vendor's security practices**
- (C) Comparing the visual appeal of the vendor's user interface to competitors
- (D) Evaluating the vendor's marketing strategies

Explanation 464. Correct Answer: B. Conducting due diligence regarding the vendor's security practices.

Conducting due diligence regarding the vendor's security practices ensures that the bank has a comprehensive understanding of the vendor's security posture and past performance, aligning with the bank's concerns for a robust and secure online transaction system.

Option A is incorrect. While a vendor's sales growth might indicate business success, it does not provide insight into their security measures.

Option C is incorrect. The visual appeal of a user interface does not provide information on the security measures or practices of a vendor.

Option D is incorrect. Evaluating marketing strategies provides no direct insight into the security practices of a vendor.

Question 465. MegaTech Inc. is in the process of outlining a strategy to ensure that after any disaster, critical applications can be restored to a working state within 4 hours. The organization also wants to make sure that the data loss does not exceed 1 hour. Which of the following policies is most relevant to achieving this objective?

- (A) Data Retention Policy
- (B) Incident Response Policy
- (C) **Disaster Recovery Policy**
- (D) Password Policy

Explanation 465. Correct Answer: C. Disaster Recovery Policy. A Disaster Recovery Policy details the strategy and procedures for recovering IT systems, applications, and data

after a catastrophic event. Defining Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) like in this scenario are essential components of this policy.

Option A is incorrect. Data Retention Policy is about how long data should be stored and when it should be discarded, not how to recover it post-disaster.

Option B is incorrect. An Incident Response Policy is centered around how to handle and respond to security incidents. While related, it does not provide the specifics on recovery objectives and timelines.

Option D is incorrect. Password Policy sets the standards for password creation and management. It doesn't have any direct relevance to disaster recovery processes.

Question 466. CyberSecure Inc. is evaluating the financial impact of a potential security breach on its main server. The company has estimated that a breach of this server would lead to a direct financial loss of \$500,000 due to data recovery, legal fees, and fines. Which of the following best represents this estimation?

- (A) Annual Rate of Occurrence (ARO)
- (B) Total Cost of Ownership (TCO)
- (C) **Single Loss Expectancy (SLE)**
- (D) Annualized Loss Expectancy (ALE)

Explanation 466. Correct Answer: C. Single Loss Expectancy (SLE). The Single Loss Expectancy (SLE) represents the expected monetary loss every time a risk occurs.

In this case, the company is estimating the direct financial loss from a single breach event.

Option A is incorrect. The Annual Rate of Occurrence (ARO) represents how often the event is expected to occur in a year, not the cost of a single event.

Option B is incorrect. Total Cost of Ownership (TCO) refers to the complete cost of owning a particular asset or solution over its lifecycle, not the cost of a single event.

Option D is incorrect. The Annualized Loss Expectancy (ALE) is a calculated value that represents the expected annual loss, based on the SLE and the ARO.

Question 467. SecureWeb LLC, a web hosting company, has experienced two server breaches over the past five years. They are currently analyzing the risks associated with their infrastructure. Which of the following best represents the Annualized Rate of Occurrence (ARO) for the server breaches?

- (A) 0.2
- (B) 0.4
- (C) 2
- (D) 5

Explanation 467. Correct Answer: B. 0.4. The Annualized Rate of Occurrence (ARO) is a measure of how often an event is expected to occur on an annual basis. Given that there have been two breaches over five years, the ARO would be 2 breaches divided by 5 years, which is 0.4.

Option A is incorrect. While it's close, the calculation for ARO should be the number of occurrences (2) divided by the number of years (5), which is 0.4, not 0.2.

Option C is incorrect. This would indicate two breaches every year, which is not the case presented.

Option D is incorrect. This would suggest that the breaches happen five times a year, which is inconsistent with the scenario.

Question 468. An e-commerce company recently faced a DDoS attack that rendered its website unavailable for several hours. While reflecting on the incident, the CISO emphasized the importance of having a detailed plan that includes identification, containment, eradication, recovery, and lessons learned. Which policy primarily encompasses these stages for handling security incidents?

- (A) Change Management Policy
- (B) **Incident Response Policy**
- (C) Disaster Recovery Policy
- (D) Remote Access Policy

Explanation 468. Correct Answer: B. Incident Response Policy. An Incident Response Policy outlines the procedures and guidelines for effectively responding to and managing security incidents. It includes various stages like identification, containment, eradication, recovery, and lessons learned to ensure a systematic approach to handling security threats.

Option A is incorrect. A Change Management Policy focuses on procedures and guidelines for making changes in the IT environment to ensure stability and security. It does not deal with responding to security incidents directly.

Option C is incorrect. The Disaster Recovery Policy pertains to recovering IT systems, applications, and data after a catastrophic event, rather than the steps for managing security incidents.

Option D is incorrect. Remote Access Policy details the guidelines for accessing the organization's network from remote locations. It doesn't provide a structured methodology for handling security incidents.

Question 469. AlphaCorp is in the final stages of selecting a cybersecurity consultant. One of the shortlisted firms, SecureWorld, recently hired AlphaCorp's former CISO as a senior consultant. Given this situation, what should be AlphaCorp's immediate concern during vendor selection?

- (A) The expertise the former CISO brings to SecureWorld
- (B) The possibility that SecureWorld could offer a discounted price
- (C) **Potential conflict of interest due to prior associations**
- (D) SecureWorld's global presence and reputation

Explanation 469. Correct Answer: C. Potential conflict of interest due to prior associations. Having the former CISO of AlphaCorp in a senior role at SecureWorld might raise concerns about potential conflicts of interest. It's essential to ensure that

decisions are made objectively, and there's no bias due to prior associations.

Option A is incorrect. While the expertise of the former CISO is valuable, it's not the primary concern in this context of potential conflict of interest.

Option B is incorrect. Pricing and discounts are not the primary concern related to potential conflicts of interest in vendor selection.

Option D is incorrect. While global presence and reputation are essential factors for vendor selection, they do not directly address the issue of potential conflict of interest arising from the former CISO's position.

Question 470. WebServ Corp., a web hosting company, has been analyzing the reliability of its servers. They found that one of their server models, on average, tends to fail once every 2000 hours and then gets promptly repaired. Which of the following metrics is WebServ Corp. evaluating?

- (A) Recovery Time Objective (RTO)
- (B) Mean Time To Repair (MTTR)
- (C) **Mean Time Between Failures (MTBF)**
- (D) Recovery Point Objective (RPO)

Explanation 470. Correct Answer: C. Mean Time Between Failures (MTBF). MTBF (Mean Time Between Failures) is a measure of how reliable hardware or a system is. It's the average time that passes from one failure to the next. For

WebServ Corp., the 2000-hour duration between failures reflects the MTBF.

Option A is incorrect. Recovery Time Objective (RTO) is the targeted time and service level within which a business process must be restored after an interruption to avoid unacceptable losses.

Option B is incorrect. Mean Time To Repair (MTTR) represents the average time needed to fix a failed component.

Option D is incorrect. Recovery Point Objective (RPO) measures the amount of data that can be lost, in terms of time, without causing harm to the business continuity.

Question 471. TechFusion Inc. is a well-established technology company that has been in the market for over 15 years.

Recently, the board of directors decided that the company will pursue aggressive growth strategies by entering new, untested markets and launching cutting-edge products, even if these strategies come with significant risks. How would you classify TechFusion Inc.'s risk appetite?

- (A) Conservative
- (B) Expansionary**
- (C) Neutral
- (D) Risk-averse

Explanation 471. Correct Answer: B. Expansionary.

Expansionary risk appetite is characterized by an entity's willingness to accept a higher level of risk in pursuit of higher rewards. Given that TechFusion Inc. is looking to enter new

markets and launch cutting-edge products, which inherently come with significant risks, their risk appetite can be classified as expansionary.

Option A is incorrect. A conservative risk appetite means an organization is very cautious and avoids taking significant risks, which is the opposite of TechFusion Inc.'s approach.

Option C is incorrect. Neutral risk appetite means an organization neither seeks to take on nor avoid risk, maintaining its current risk position.

Option D is incorrect. Risk-averse is similar to conservative, where an organization is very cautious about taking on new risks. It doesn't capture the aggressive growth strategy described.

Question 472. After a significant merger between two large corporations, a comprehensive risk assessment was conducted to identify potential security gaps within the combined infrastructure. This assessment was exclusive to the merger and was not planned to be repeated in the future. What type of risk assessment was this?

- (A) Recurring
- (B) Continuous
- (C) **One-time**
- (D) Dynamic

Explanation 472. Correct Answer: C. One-time. A one-time risk assessment is a unique assessment carried out for a specific

purpose or event, such as a merger, and is not repeated regularly like other types of assessments.

Option A is incorrect. Recurring risk assessments are conducted at regular intervals, such as annually or biannually.

Option B is incorrect. Continuous risk assessments involve ongoing monitoring of risks and do not refer to a single, specific assessment.

Option D is incorrect. Dynamic assessments continuously adapt to changing environments or factors, but this term does not denote a single, specific assessment.

Question 473. AcmeTech, a software development firm, recently experienced a major data breach that was traced back to a vulnerability in their custom-built application. Post-incident analysis revealed that the vulnerability had been introduced during the coding phase and was never detected during testing. To avoid such vulnerabilities in the future, which policy should AcmeTech emphasize to ensure secure practices are maintained throughout the development process?

- (A) Incident Response Policy
- (B) Change Management Policy
- (C) Business Continuity Policy
- (D) **Software Development Lifecycle (SDLC) Policy**

Explanation 473. Correct Answer: D. Software Development Lifecycle (SDLC) Policy. The Software Development Lifecycle (SDLC) Policy provides guidelines and standards for each phase of the software development process, ensuring that

security is integrated at every step, from requirement gathering to deployment and maintenance.

Option A is incorrect. While an Incident Response Policy provides a structured approach to manage and respond to security incidents, it does not focus on the software development process.

Option B is incorrect. The Change Management Policy deals with procedures for implementing changes in the IT environment but doesn't specifically cater to the development of software applications.

Option C is incorrect. A Business Continuity Policy focuses on maintaining business operations during and after a disruption and doesn't address the specifics of software development.

Question 474. An organization is conducting a risk assessment for its cloud infrastructure. The assessment has determined that the likelihood of a data breach through an insecure API is "High." What factors may have contributed to this likelihood rating?

(A) The API has been thoroughly tested and has a known secure configuration

(B) There are few records of this kind of breach in the industry

(C) **The API is publicly accessible and has had several vulnerabilities reported in the past six months**

(D) The cloud provider offers a guaranteed SLA against any form of security breach

Explanation 474. Correct Answer: C. The API is publicly accessible and has had several vulnerabilities reported in the past six months. A publicly accessible API with a history of recent vulnerabilities significantly increases the likelihood of a breach, making this scenario the best fit for a “High” likelihood rating.

Option A is incorrect. A thoroughly tested and known secure configuration would likely reduce the likelihood rating.

Option B is incorrect. Few records of similar breaches would also likely reduce the assessed likelihood.

Option D is incorrect. A guaranteed SLA might offer remedies post-breach, but it does not inherently reduce the likelihood of a breach occurring.

Question 475. SecureNet Ltd. wants to protect user accounts from brute force attacks. They want to implement a measure where, after a certain number of failed login attempts, the account would become temporarily inaccessible. Which standard best suits this requirement?

- (A) Password minimum length
- (B) **Account lockout threshold**
- (C) Mandatory password resets
- (D) Two-factor authentication

Explanation 475. Correct Answer: B. Account lockout threshold. The account lockout threshold defines the number of consecutive failed login attempts after which a user account is locked out, preventing further attempts for a specified duration.

This measure directly deters brute force attacks by making rapid, repeated login attempts unfeasible.

Option A is incorrect. Password minimum length dictates how long a password must be, which can deter certain brute force attempts but doesn't address the rapid, repeated attempts characteristic of such attacks.

Option C is incorrect. Mandatory password resets force users to change their passwords at regular intervals. While this might protect against the use of older stolen credentials, it doesn't prevent brute force attacks.

Option D is incorrect. Two-factor authentication requires two forms of identification to access an account. Although it significantly enhances security, it doesn't limit login attempts based on failed attempts.

Question 476. After a recent security breach, CyberSolutions Inc. evaluated their response metrics and determined that, on average, it took 4 hours from identifying a security breach to having it completely resolved. Which metric best describes this 4-hour timeframe?

- (A) Recovery Time Objective (RTO)
- (B) Recovery Point Objective (RPO)
- (C) Mean Time Between Failures (MTBF)
- (D) **Mean Time To Repair (MTTR)**

Explanation 476. Correct Answer: D. Mean Time To Repair (MTTR). MTTR (Mean Time To Repair) is a basic measure of the maintainability of repairable items. It represents the average

time required to repair a failed component or device. For CyberSolutions Inc., the 4-hour duration from identifying to resolving the breach reflects the MTTR.

Option A is incorrect. Recovery Time Objective (RTO) is the targeted duration of time within which a business process must be restored after a disaster to avoid unacceptable consequences.

Option B is incorrect. Recovery Point Objective (RPO) represents the maximum acceptable amount of data loss measured in time.

Option C is incorrect. Mean Time Between Failures (MTBF) is the predicted elapsed time between inherent failures of a mechanical or electronic system, during normal system operation.

Question 477. SecureCom, a telecommunications company, is planning to expand its infrastructure across Country A. The nation recently updated its telecommunications regulations and mandates strict guidelines for all external communications. Which of the following should be SecureCom's primary focus as it begins its expansion?

- (A) Increasing advertising budget to gain a stronger market presence in Country A
- (B) **Ensuring its infrastructure meets the national standards for secure and encrypted communications**
- (C) Collaborating with local tech companies to better understand the culture of Country A
- (D) Launching new products tailored to the preferences of Country A's residents

Explanation 477. Correct Answer: B. Ensuring its infrastructure meets the national standards for secure and encrypted communications. Telecommunication companies, by their nature, handle vast amounts of data and communication traffic. As such, when a nation mandates specific security guidelines for external communications, companies like SecureCom must ensure their infrastructure complies with those guidelines to avoid legal and financial repercussions.

Option A is incorrect. While advertising is essential for market growth, the primary concern when expanding infrastructure in a country with strict telecommunications regulations should be compliance.

Option C is incorrect. Collaborating with local tech companies can offer insights into the local market, but regulatory compliance should remain the primary focus, especially given the updated regulations.

Option D is incorrect. Launching tailored products is a sound business strategy, but without ensuring compliance with national regulations, the company might face significant challenges.

Question 478. During an audit review at NetSecure Corp., the external auditors observed that the company is willing to take risks that can potentially result in a 10% decrease in their annual profits, but no more than that. The auditors want to document this finding in their report. Which term should they use to describe NetSecure Corp.'s stance?

(A) Risk Avoidance

- (B) Risk Transfer
- (C) **Risk Tolerance**
- (D) Risk Assessment

Explanation 478. Correct Answer: C. Risk Tolerance. Risk tolerance represents the maximum amount of risk an entity is willing to accept or tolerate. NetSecure Corp.'s acceptance of risks that can result in up to a 10% decrease in annual profits represents their risk tolerance level.

Option A is incorrect. Risk avoidance means completely sidestepping any activities that have associated risks. The scenario indicates that the company is willing to take risks, but within certain limits.

Option B is incorrect. Risk transfer involves offloading certain risks to other parties, typically through insurance or other contractual methods. The scenario doesn't provide information about transferring risks.

Option D is incorrect. Risk assessment is the overall process of identifying, analyzing, and evaluating risks. The scenario is more focused on the company's willingness to accept a specific level of risk rather than assessing it.

Question 479. TechGuard Corp. conducts a risk assessment every six months to identify new vulnerabilities and ensure that previous risk-mitigation strategies remain effective. This type of risk assessment is best described as:

- (A) Periodic
- (B) Ad hoc

- (C) Continuous
- (D) **Recurring**

Explanation 479. Correct Answer: D. Recurring. Recurring risk assessments are those that are conducted at regular intervals, such as quarterly, biannually, or annually, to continually identify, review, and address vulnerabilities and threats.

Option A is incorrect. While “periodic” might sound similar to “recurring”, in the context of risk assessments, the term “recurring” more accurately describes assessments that are conducted regularly at defined intervals.

Option B is incorrect. Ad hoc risk assessments are done in response to a specific event or situation and are not planned in advance.

Option C is incorrect. Continuous risk assessments involve constant or ongoing monitoring of risks, rather than taking place at set intervals.

Question 480. CyberFleet Inc., a software development company, has just heard of a newly discovered vulnerability in a third-party library they heavily rely upon. The security team quickly gathers to understand and analyze the potential risks associated with this vulnerability. This spontaneous assessment is best described as:

- (A) Routine
- (B) **Ad hoc**

- (C) Scheduled
- (D) Benchmark

Explanation 480. Correct Answer: B. Ad hoc. An ad hoc risk assessment is done in response to a specific event or situation and is not planned in advance.

Option A is incorrect. Routine assessments, similar to periodic ones, are performed at regular intervals and are not typically in response to sudden events.

Option C is incorrect. Scheduled risk assessments are planned and occur at predetermined times or intervals.

Option D is incorrect. Benchmark assessments are evaluations that compare an organization's processes or performance against a set standard or best practices in the industry.

Question 481. TechFlow Corp. is undergoing a risk analysis for its online platform. If a critical vulnerability were exploited, the company would have to pay \$10,000 in repair costs, \$5,000 in compensation to customers, and a \$15,000 fine to regulatory bodies. What would be the Single Loss Expectancy (SLE) for this vulnerability?

- (A) \$10,000
- (B) \$20,000
- (C) **\$30,000**
- (D) \$50,000

Explanation 481. Correct Answer: C. \$30,000. Single Loss Expectancy (SLE) is the cost of a single event or incident. In

this scenario, adding up the repair costs, compensations, and fines gives: $\$10,000 + \$5,000 + \$15,000 = \$30,000$.

Option A is incorrect. This only accounts for the repair costs.

Option B is incorrect. This only considers the repair costs and compensations but omits the fines.

Option D is incorrect. This value exceeds the combined costs from the vulnerability being exploited.

Question 482. GlobalTech, a multinational corporation, is negotiating a cloud storage contract with CloudCorp. GlobalTech wants to ensure that data retrieval times remain under 2 seconds 99.9% of the time. Which component should be explicitly defined in their agreement to set this expectation?

- (A) Pricing model
- (B) Data sovereignty clauses
- (C) **Service-level agreement (SLA)**
- (D) Termination clauses

Explanation 482. Correct Answer: C. Service-level agreement (SLA). Service-level agreements (SLAs) are designed to define specific metrics, responsibilities, and expectations to ensure that both parties understand and agree to the performance benchmarks and consequences if those benchmarks are not achieved. In this scenario, the SLA would specify the expected data retrieval times.

Option A is incorrect. While pricing is an essential aspect of any contract, it does not specify performance expectations like data retrieval times.

Option B is incorrect. Data sovereignty clauses pertain to the legal aspects of where data is stored and processed, not to performance metrics.

Option D is incorrect. Termination clauses deal with the conditions under which the agreement might be terminated, not with performance expectations.

Question 483. A software development company is evaluating the risks associated with a newly discovered vulnerability in its application. After reviewing logs and simulating potential attacks, the security team estimates that there is a 0.25 probability of the vulnerability being exploited in the next year. What does this probability indicate?

- (A) The vulnerability has a 1 in 4 chance of being exploited in the next year
- (B) The vulnerability will certainly be exploited four times in the next year
- (C) The vulnerability has been exploited 25 times in the past year
- (D) Every fourth customer will exploit the vulnerability.

Explanation 483. Correct Answer: A. The vulnerability has a 1 in 4 chance of being exploited in the next year. A probability of 0.25 indicates a 25% chance, or a 1 in 4 likelihood, of an event occurring.

Option B is incorrect. A probability value doesn't predict a definite number of occurrences, just the likelihood of an occurrence.

Option C is incorrect. The probability figure given is an estimate of future risk, not a tally of past events.

Option D is incorrect. The probability provided is not about customers but about the chance of the vulnerability being exploited.

Question 484. A global e-commerce company maintains a risk register to keep track of identified risks and to monitor specific metrics that might indicate an increased risk level. Recently, there has been a 20% increase in abandoned shopping carts on their platform. How should this metric be categorized in the context of the risk register?

- (A) Risk Appetite
- (B) Risk Mitigation Strategy
- (C) **Key Risk Indicator (KRI)**
- (D) Risk Tolerance Threshold

Explanation 484. Correct Answer: C. Key Risk Indicator (KRI). Key Risk Indicators (KRIs) are metrics used to measure and provide an early signal of increasing risk exposures in various areas of an organization. In this scenario, the 20% increase in abandoned shopping carts can serve as a KRI, signaling potential issues like site performance, security concerns, or user experience that may need to be addressed.

Option A is incorrect. Risk appetite refers to the amount of risk an organization is willing to accept in pursuit of its objectives. The increase in abandoned carts doesn't measure this.

Option B is incorrect. A risk mitigation strategy describes actions an organization plans to take to address risks. The metric provided is a measure, not an action or strategy.

Option D is incorrect. Risk tolerance threshold indicates the amount of risk an organization is willing to tolerate. The scenario describes a metric that might indicate an issue, not a predefined threshold.

Question 485. A financial institution has reported that they experience an average of 3 phishing attacks every year that attempt to compromise their user data. Based on this data, what is the Annualized Rate of Occurrence (ARO) for these phishing attacks?

- (A) 0.33
- (B) 1
- (C) 3
- (D) 12

Explanation 485. Correct Answer: C. 3. The Annualized Rate of Occurrence (ARO) represents the expected frequency of a specific event or risk occurring each year. Given that the financial institution experiences 3 phishing attacks every year, the ARO is 3.

Option A is incorrect. An ARO of 0.33 would indicate that the event happens approximately once every three years, not thrice in a year.

Option B is incorrect. An ARO of 1 would suggest the event happens once a year, which is not consistent with the scenario.

Option D is incorrect. This would indicate the event occurs 12 times a year or once a month, which is not the case based on the information provided.

Question 486. During a board meeting at DataFlow Corp., the CEO emphasizes that while they are willing to take certain risks for innovation, there's a limit to the amount of risk they are willing to take, especially concerning potential financial losses. To ensure that risks stay below this level, what should be defined in the risk register?

- (A) Risk Owner Assignment
- (B) Key Risk Indicator (KRI)
- (C) Risk Impact Analysis
- (D) **Risk Threshold**

Explanation 486. Correct Answer: D. Risk Threshold. The risk threshold indicates the maximum level of risk an organization is willing to tolerate or accept. Setting a clear risk threshold ensures that any risks that surpass this level are given priority for management or mitigation.

Option A is incorrect. While assigning a Risk Owner is crucial for accountability, it doesn't define the maximum level of risk an organization is willing to tolerate.

Option B is incorrect. A Key Risk Indicator (KRI) provides early signals of increasing risk exposures. While they are essential for monitoring risks, they don't establish the maximum tolerable risk level.

Option C is incorrect. Risk Impact Analysis assesses the potential consequences of a given risk but doesn't set a level indicating the maximum risk the organization is prepared to accept.

Question 487. XYZ Corporation recently implemented a security solution that constantly evaluates the company's threat landscape, monitoring for emerging risks and immediately alerting the security team of any changes. This assessment model allows the team to rapidly adapt their security posture in response to live threats. What type of risk assessment is XYZ Corporation utilizing?

- (A) One-time
- (B) Periodic
- (C) Dynamic
- (D) **Continuous**

Explanation 487. Correct Answer: D. Continuous.

Continuous risk assessments involve ongoing and real-time monitoring of risks, enabling an organization to instantly react to emerging threats and vulnerabilities.

Option A is incorrect. A one-time risk assessment is specific to a single event or purpose and is not intended to be repeated regularly.

Option B is incorrect. Periodic risk assessments are carried out at scheduled intervals, such as annually or biannually, and are not ongoing.

Option C is incorrect. Dynamic assessments can adapt to changing environments or factors, but “dynamic” doesn’t specifically denote ongoing, real-time assessment like “continuous” does.

Question 488. Your organization is considering a partnership with TechVendor Inc., a software solution provider. Before finalizing the agreement, you wish to ensure their application’s security. What would be the most direct method to assess the robustness of their system against potential cyber threats?

- (A) Conducting an internal security awareness training
- (B) Reviewing their past audit reports
- (C) Implementing strict firewall rules
- (D) **Performing a penetration test on their application.**

Explanation 488. Correct Answer: D. Performing a penetration test on their application. Penetration testing is a proactive method used to evaluate the security of an application by simulating an attack from malicious outsiders or insiders. It provides a direct measure of the vulnerabilities present in the application that could potentially be exploited by an attacker.

Option A is incorrect. While security awareness training is crucial for educating staff about security best practices, it does not directly assess the security of an external vendor’s application.

Option B is incorrect. Past audit reports can provide valuable insights into a vendor's security posture, but they do not offer real-time assessment like penetration testing.

Option C is incorrect. Implementing firewall rules is a protective measure, but it does not evaluate the current security of the vendor's application.

Question 489. MedGuard, a health tech company, has developed an AI-driven software that predicts potential health risks based on patient data. Before launching in the U.S. market, which of the following industry external considerations should be the company's primary focus?

- (A) Integrating with popular fitness tracking apps in the U.S.
- (B) Ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA)**
- (C) Surveying U.S. doctors about software interface preferences
- (D) Collaborating with U.S. pharmaceutical companies for promotional deals

Explanation 489. Correct Answer: B. Ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA). HIPAA is a U.S. law designed to provide privacy standards to protect patients' medical records and other health information. For MedGuard, which deals with patient data, ensuring HIPAA compliance is paramount before launching their software in the U.S. market.

Option A is incorrect. While integration with fitness tracking apps may enhance the software's functionality, the primary concern when dealing with patient data in the U.S. is compliance with HIPAA.

Option C is incorrect. Although feedback from doctors might help improve the software's user interface, the primary industry external consideration should be regulatory compliance, especially when handling sensitive health information.

Option D is incorrect. While partnerships with pharmaceutical companies might be beneficial for marketing or business growth, the primary industry consideration for a health tech company dealing with patient data is ensuring compliance with relevant regulations.

Question 490. During a company's onboarding process, new employees are required to read and acknowledge understanding of various company policies. The HR department wants to ensure that employees are aware of their responsibilities when it comes to the use of company devices and internet resources. Which policy should be included in the onboarding packet to address this?

- (A) Password Complexity Policy
- (B) Data Classification Policy
- (C) **Acceptable Use Policy (AUP)**
- (D) Vendor Management Policy

Explanation 490. Correct Answer: C. Acceptable Use Policy (AUP). The Acceptable Use Policy (AUP) outlines the do's and don'ts for employees regarding the use of company devices,

networks, and other IT resources. Including this in the onboarding packet will ensure that new hires are aware of their responsibilities.

Option A is incorrect. While important, the Password Complexity Policy primarily deals with the requirements for creating and managing passwords, not the overall acceptable use of IT resources.

Option B is incorrect. A Data Classification Policy focuses on the categorization of data based on its sensitivity. It doesn't provide guidelines on the acceptable use of IT resources.

Option D is incorrect. The Vendor Management Policy governs the relationship and security expectations between the company and its vendors, not the acceptable use of company IT resources by employees.

Question 491. XYZ Corp is in the process of defining clear roles and responsibilities for their IT assets. During a meeting, the team discussed the primary individual who will have the responsibility for the data within a specific IT system and also be the main point of contact for any decisions related to it. Which of the following roles best describes this individual?

- (A) System administrator
- (B) Data custodian
- (C) **System owner**
- (D) End-user

Explanation 491. Correct Answer: C. System owner. The system owner, sometimes known as the data owner, is typically

responsible for the data within a specific IT system. They have the primary responsibility for ensuring the confidentiality, integrity, and availability of the data and act as the main point of contact for decisions related to that system.

Option A is incorrect. A system administrator is responsible for the daily management, operations, and support of IT systems but doesn't usually make high-level decisions about the data contained within them.

Option B is incorrect. A data custodian is typically responsible for implementing the controls and processes as defined by the data owner. They may handle the practical aspects of data management, but they don't usually make overarching decisions about the data.

Option D is incorrect. An end-user utilizes the data or system for their job function but doesn't typically have decision-making responsibilities regarding the data's overall management and protection.

Question 492. As the Chief Security Officer (CSO) of AlphaTech, you are in the process of finalizing a partnership agreement with a third-party provider. To ensure ongoing security compliance and transparency, you want to reserve the right for your organization to inspect the vendor's operations and security measures in the future. Which clause should you ensure is included in the contract?

- (A) Non-disclosure agreement (NDA)
- (B) Service level agreement (SLA)

- (C) Termination clause
- (D) **Right-to-audit clause**

Explanation 492. Correct Answer: D. Right-to-audit clause.

The right-to-audit clause allows an organization to review or audit a vendor's procedures, systems, records, and practices to ensure they comply with agreed-upon security and privacy requirements.

Option A is incorrect. While an NDA is essential to protect confidential information, it doesn't give an organization the right to audit a vendor's practices.

Option B is incorrect. An SLA sets expectations around the quality and availability of services provided, but it doesn't pertain to the right to audit.

Option C is incorrect. A termination clause defines the conditions under which a partnership can be ended, but it doesn't grant audit rights.

Question 493. CyberGuard LLC, a cybersecurity firm, is in a stable position in its industry with consistent returns. The leadership decides not to pursue aggressive growth strategies but instead chooses to maintain its current market share and operational scale. They are open to minor risks but avoid major disruptions. How can one best describe CyberGuard LLC's risk appetite?

- (A) Expansionary
- (B) **Neutral**

- (C) Conservative
- (D) Aggressive

Explanation 493. Correct Answer: B. Neutral. A neutral risk appetite means an organization is neither aggressively pursuing risks for high rewards nor entirely avoiding them. Given that CyberGuard LLC is looking to maintain its current position and is open to minor risks, their risk appetite can be classified as neutral.

Option A is incorrect. Expansionary risk appetite denotes an organization's willingness to accept higher risks to achieve potentially higher rewards, which doesn't align with CyberGuard LLC's strategy.

Option C is incorrect. While CyberGuard LLC is cautious, their stance is not entirely against taking risks. A conservative appetite would imply they avoid most risks, but they are open to minor ones.

Option D is incorrect. Aggressive would imply a strong willingness to take on significant risks, which is not the stance described for CyberGuard LLC.

Question 494. Two university research departments, UniAlpha and UniBeta, decide to collaborate on a project exploring quantum computing's security implications. They need an agreement to express mutual intentions without enforcing legally binding obligations. Which document is most suitable for their needs?

- (A) Service-level agreement (SLA)

- (B) Non-disclosure agreement (NDA)
- (C) **Memorandum of understanding (MOU)**
- (D) Licensing agreement

Explanation 494. Correct Answer: C. Memorandum of understanding (MOU). A Memorandum of Understanding (MOU) serves as a formal agreement between parties to signal mutual intentions without necessarily introducing legally binding terms. Given that UniAlpha and UniBeta want to signify their shared intentions on a collaborative research project, an MOU is the most appropriate choice.

Option A is incorrect. An SLA is typically between a service provider and a customer and details the level of service expected.

Option B is incorrect. An NDA focuses on the confidentiality of information shared between parties.

Option D is incorrect. A licensing agreement concerns the rights to use, distribute, or reproduce software or intellectual property.

Question 495. TechFirm is preparing to embark on a new project with a client, focusing on implementing a cybersecurity infrastructure overhaul. They wish to lay out the specific tasks, deliverables, timelines, and resources required for this project. Which type of agreement would best capture these details?

- (A) Memorandum of understanding (MOU)
- (B) Joint venture agreement

- (C) Master service agreement (MSA)
- (D) **Work order (WO)/statement of work (SOW)**

Explanation 495. Correct Answer: D. Work order (WO)/statement of work (SOW). A Work order (WO) or statement of work (SOW) is tailored to outline the specifics of a particular job or project. It often includes details such as tasks, deliverables, schedules, and necessary resources. Given that TechFirm seeks to describe the details of their cybersecurity overhaul project, the WO/SOW is the most appropriate choice.

Option A is incorrect. An MOU is a more general agreement signifying mutual intentions, but it doesn't delve into specific tasks or deliverables of a particular project.

Option B is incorrect. A joint venture agreement is mainly concerned with the creation of a new entity or project involving multiple parties, highlighting their roles and responsibilities.

Option C is incorrect. A Master service agreement (MSA) provides a broad framework covering the terms and conditions of business transactions between parties. It doesn't specify details of individual projects.

Question 496. AcmeBank recently performed a business impact analysis for its online banking system. The result indicated that the bank could tolerate a maximum downtime of 4 hours for the system before incurring significant financial losses and customer dissatisfaction. Which concept best describes this 4-hour period?

- (A) Recovery Point Objective (RPO)

- (B) Maximum Tolerable Downtime (MTD)
- (C) **Recovery Time Objective (RTO)**
- (D) Time To Restore (TTR)

Explanation 496. Correct Answer: C. Recovery Time Objective (RTO). The Recovery Time Objective (RTO) is the targeted duration of time within which a business process must be restored after a disruption in order to avoid unacceptable consequences. In this scenario, AcmeBank's RTO for its online banking system is 4 hours.

Option A is incorrect. Recovery Point Objective (RPO) describes the maximum age of files that an organization must recover from backup storage for normal operations to resume after a disaster. It doesn't refer to the time duration.

Option B is incorrect. Maximum Tolerable Downtime (MTD) is the longest period of time that a business process can be down before causing irreparable harm to the business. While related, the question specifically describes the RTO.

Option D is incorrect. Time To Restore (TTR) is often a metric to measure the time it takes to restore a particular process or system. However, the scenario directly describes an RTO.

Question 497. DigitalZone Corp, a marketing company, collects personal data from users and determines how and why that data will be processed. At the same time, they engage an external company, CloudSolutions, to store and manage this data. In this scenario, what role does DigitalZone Corp play in relation to data protection regulations?

- (A) Processor
- (B) Data subject
- (C) **Controller**
- (D) Third-party provider

Explanation 497. Correct Answer: C. Controller. DigitalZone Corp makes decisions about how and why the data is processed, which means they play the role of the controller in the context of data protection regulations.

Option A is incorrect. The processor is the entity that processes personal data on behalf of the controller. In this scenario, CloudSolutions acts as the processor as they are storing and managing the data for DigitalZone Corp.

Option B is incorrect. The data subject is the individual whose personal data is being collected. It's not an entity that makes decisions about the data or processes it.

Option D is incorrect. While CloudSolutions could be considered a third-party provider, this term is broader and does not specifically refer to an entity's role in data protection terms as a controller or processor.

Question 498. TechFirm Inc. has decided to engage in a new business venture. Before they move forward, the security team conducts several brainstorming sessions, interviews, and reviews historical data to generate a list of potential security threats that the new venture could face. This activity is a primary component of which step in the risk management process?

- (A) Risk assessment
- (B) Risk response
- (C) Risk monitoring
- (D) **Risk identification**

Explanation 498. Correct Answer: D. Risk identification.

Risk identification is the initial process of detecting and describing risks that could potentially affect the achievement of objectives.

Option A is incorrect. Risk assessment encompasses the overall process of identifying, analyzing, and evaluating risks, but the specific activity mentioned is related to risk identification.

Option B is incorrect. Risk response involves deciding on the most suitable approach to address identified risks, whether it's accepting, avoiding, transferring, or mitigating them.

Option C is incorrect. Risk monitoring is about tracking identified risks, monitoring residual risks, and identifying new risks. The specific activity of brainstorming and gathering data about risks falls under risk identification.

Question 499. A healthcare organization uses a software platform to manage patient records. A recent vulnerability assessment identified a potential exploit where an unauthorized individual might gain access to 30% of stored patient data. Which of the following BEST describes this scenario?

- (A) The threat likelihood is 30%
- (B) The vulnerability has a 30% rate of occurrence

- (C) The exposure factor of the vulnerability is 30%
- (D) 30% of the patients have been impacted

Explanation 499. Correct Answer: C. The exposure factor of the vulnerability is 30%. The exposure factor is a measure of the magnitude of loss or percentage of asset value that a realized threat would destroy or damage. In this case, the vulnerability could lead to 30% of patient data being accessed.

Option A is incorrect. Likelihood refers to the probability of an event happening, not the potential impact or amount of data that might be exposed.

Option B is incorrect. The rate of occurrence (ARO) is a measure of how often a specific event will occur, not the potential impact or amount of data that might be exposed.

Option D is incorrect. The scenario does not indicate that 30% of patients have already been impacted, only that their data might be accessed if the vulnerability is exploited.

Question 500. XYZ Corporation recently faced a major power outage that affected their primary data center. During the incident, it was found that there was no clear guidance on the steps to maintain or quickly restore business operations. To address this, which of the following policies should XYZ Corporation prioritize implementing?

- (A) Data Classification Policy
- (B) **Business Continuity Policy**
- (C) Acceptable Use Policy
- (D) Network Segmentation Strategy

Explanation 500. Correct Answer: B. Business Continuity

Policy. A Business Continuity Policy outlines the processes and procedures an organization should follow to ensure that essential functions can continue during and after a disaster. It provides a roadmap for maintaining and quickly restoring business operations.

Option A is incorrect. The Data Classification Policy is concerned with categorizing data based on its sensitivity but doesn't address continuity of business operations during disruptions.

Option C is incorrect. The Acceptable Use Policy specifies how the organization's IT resources and networks can be used by employees. It doesn't provide guidance on restoring business operations during a disaster.

Option D is incorrect. While Network Segmentation Strategy is crucial for security, dividing the network into segments does not specifically address business continuity during major disruptions.

Question 501. AlphaTech wants to ensure that its remote employees follow best security practices when working from home. The security team has been tasked with drafting a set of guidelines for remote work. What should be the primary focus of these guidelines?

- (A) Outlining punitive measures for non-compliance
- (B) Stating the company's legal position on remote work
- (C) **Recommending security measures for home networks and devices**

(D) Dictating the exact software and hardware specifications for remote workers

Explanation 501. Correct Answer: C. Recommending security measures for home networks and devices.

Guidelines aim to provide advice and recommendations. In the context of remote work, they would suggest best security practices for securing home networks and devices without being overly prescriptive.

Option A is incorrect. Punitive measures and compliance repercussions are typically outlined in policies or procedures, not guidelines.

Option B is incorrect. The company's legal position on remote work would be part of a policy or a legal document rather than a set of guidelines.

Option D is incorrect. Dictating exact software and hardware specifications would be more in line with standards rather than guidelines. Guidelines would provide broader recommendations.

Question 502. Lisa, a security manager, is reviewing the company's existing policies and realizes that there isn't a comprehensive document detailing the organization's stance, expectations, and commitment to protecting its information assets. Which of the following should Lisa prioritize creating to address this gap?

(A) Incident Response Plan

(B) Information Security Policy

- (C) Acceptable Use Policy
- (D) Data Backup Strategy

Explanation 502. Correct Answer: B. Information Security Policy. An Information Security Policy is a foundational document that provides a framework for information security throughout the organization. It encompasses the organization's vision, principles, and responsibilities regarding the protection of its data and IT assets.

Option A is incorrect. An Incident Response Plan focuses on the steps to be taken after a security incident has occurred. It does not detail the overall stance of an organization on information security.

Option C is incorrect. An Acceptable Use Policy provides guidelines on how employees should use company resources, but it doesn't provide a comprehensive overview of an organization's commitment to protecting its information assets.

Option D is incorrect. While a Data Backup Strategy is crucial for data availability and recovery, it does not convey the broader perspective and commitment of the organization to information security.

Question 503. TechFusion and CodeRush, two independent software development companies, are collaborating on a project that is expected to define industry standards for a new coding language. While both parties have an understanding of shared responsibilities, they have not yet established legally binding obligations. Which type of agreement best suits their current

collaborative understanding?

- (A) Service-level agreement (SLA)
- (B) Non-disclosure agreement (NDA)
- (C) **Memorandum of agreement (MOA)**
- (D) Licensing agreement

Explanation 503. Correct Answer: C. Memorandum of agreement (MOA). A Memorandum of Agreement (MOA) outlines mutual understandings and responsibilities between two or more parties and does not necessarily contain legally binding obligations. In this scenario, TechFusion and CodeRush have a shared understanding but have not reached legally binding terms, making an MOA the most appropriate choice.

Option A is incorrect. An SLA specifies performance metrics and expectations between a service provider and a customer. It doesn't necessarily suit a collaborative project aiming to define industry standards.

Option B is incorrect. An NDA pertains to the confidentiality of information and would not define mutual understandings or responsibilities related to project collaboration.

Option D is incorrect. A licensing agreement typically deals with the rights to use, distribute, or reproduce software or intellectual property.

Question 504. As part of improving their security posture, TechHive Inc. decided to review their existing password policies. The current policy requires employees to use at least one uppercase letter, one number, and one special character.

However, they found that users mostly only make minimal changes to their passwords during resets. Which standard should be integrated into their policy to ensure passwords are more complex and unique over time?

- (A) **Password history retention**
- (B) Password expiration period
- (C) Account lockout duration
- (D) Maximum password age

Explanation 504. Correct Answer: A. Password history retention. Password history retention ensures that users cannot reuse a certain number of previous passwords, forcing them to come up with unique passwords rather than making only minor changes to their current ones.

Option B is incorrect. The password expiration period dictates how long a password is valid before prompting the user for a change. While it can make users change passwords frequently, it doesn't prevent them from making minimal changes.

Option C is incorrect. Account lockout duration specifies the time an account remains locked after a predefined number of incorrect login attempts. It doesn't ensure password complexity or uniqueness over time.

Option D is incorrect. Maximum password age defines how long a password can be used before it must be changed. Like Option B, it doesn't prevent users from making minimal changes to their passwords.

Question 505. CyberTech Inc., a cybersecurity consulting company, is in discussions with a potential client, MedCorp, to assist in developing a new secure medical records system. MedCorp will be sharing sensitive patient data with CyberTech as part of the process. Which agreement should be in place before the sharing of such information to ensure confidentiality?

- (A) Memorandum of understanding (MOU)
- (B) Service-level agreement (SLA)
- (C) **Non-disclosure agreement (NDA)**
- (D) Work order (WO)/statement of work (SOW)

Explanation 505. Correct Answer: C. Non-disclosure agreement (NDA). An NDA (Non-disclosure agreement) is specifically designed to safeguard confidential information that is shared between two parties. It ensures that the receiving party doesn't disclose or misuse the information provided. Given the sensitive nature of the patient data that MedCorp will share, an NDA is crucial.

Option A is incorrect. An MOU signifies mutual intentions and understanding between parties but doesn't specifically cater to the confidentiality of shared information.

Option B is incorrect. A service-level agreement (SLA) is primarily about the level of service to be provided, detailing performance metrics, and penalties for non-compliance. It doesn't inherently focus on data confidentiality.

Option D is incorrect. A Work order (WO) or statement of work (SOW) details the specifics of a project, from tasks to

milestones, but doesn't directly address the confidentiality of shared data.

Question 506. AlphaTech is conducting a risk analysis on their new online payment gateway. They've calculated the Annual Rate of Occurrence (ARO) for a specific vulnerability as 2, and the Single Loss Expectancy (SLE) as \$50,000. How much should AlphaTech anticipate losing annually due to this vulnerability?

- (A) \$10,000
- (B) **\$100,000**
- (C) \$25,000
- (D) \$1,000,000

Explanation 506. Correct Answer: B. \$100,000. The Annualized Loss Expectancy (ALE) is calculated by multiplying the Annual Rate of Occurrence (ARO) by the Single Loss Expectancy (SLE). In this scenario, $ALE = 2 \times \$50,000 = \$100,000$.

Option A is incorrect. This does not correctly apply the formula for ALE.

Option C is incorrect. This is half of the Single Loss Expectancy and does not represent an annual loss.

Option D is incorrect. This amount is significantly higher than the calculated ALE.

Question 507. WhiteCape Healthcare, an international healthcare provider, has a large patient database that includes

many EU citizens. They're about to implement a new system to improve data access for physicians. Which of the following regulatory requirements should they pay particular attention to when granting physicians access to EU patient data?

- (A) Ensure data is only accessed for tax reporting purposes
- (B) Acquire explicit consent from patients before sharing data**
- (C) Encrypt all data using a proprietary algorithm
- (D) Store data in a physical server located within the EU

Explanation 507. Correct Answer: B. Acquire explicit consent from patients before sharing data. Under the GDPR, explicit consent from individuals is required before processing or sharing their personal data. This means that EU citizens should have given their clear permission for their data to be accessed and shared.

Option A is incorrect. Accessing data for tax reporting purposes is not directly related to the GDPR's requirement for handling EU citizens' personal healthcare data.

Option C is incorrect. While encryption is a good practice for data protection, GDPR does not mandate using a proprietary algorithm. Moreover, encryption alone doesn't address the consent requirement.

Option D is incorrect. While the GDPR does have provisions about data transfer outside the EU, simply storing data in a physical server within the EU does not bypass the need for explicit patient consent when sharing their data.

Question 508. WebFlix, a popular online movie streaming service, experienced a data center outage due to a natural disaster. They had backups in place and restored their systems using data from 6 hours prior to the outage. This resulted in the loss of some user interactions, like ratings and watchlists from the last 6 hours. What term describes the 6-hour gap between the last backup and the time of the outage?

- (A) Recovery Time Objective (RTO)
- (B) Maximum Tolerable Downtime (MTD)
- (C) Recovery Duration Period (RDP)
- (D) **Recovery Point Objective (RPO)**

Explanation 508. Correct Answer: D. Recovery Point Objective (RPO). The Recovery Point Objective (RPO) is the maximum acceptable amount of data loss measured in time. For WebFlix, this means they could afford to lose up to 6 hours of data (user interactions in this case) in the event of a disaster.

Option A is incorrect. Recovery Time Objective (RTO) is the maximum acceptable amount of time that a system can be down after a disruption.

Option B is incorrect. Maximum Tolerable Downtime (MTD) represents the total amount of time a system can afford to be non-operational without incurring significant risks or significant losses.

Option C is incorrect. Recovery Duration Period (RDP) is not a standard term in business continuity and disaster recovery planning.

Question 509. As a security consultant, you are hired by a multinational corporation to assess the security posture of their potential vendors. One of the vendors appears promising, but your client wants to ensure that the vendor periodically examines and strengthens its own internal procedures and security controls. What should you advise your client to request from this vendor?

- (A) The vendor's business continuity plan
- (B) A list of the vendor's clients
- (C) **Evidence of internal audits**
- (D) The vendor's company mission statement

Explanation 509. Correct Answer: C. Evidence of internal audits. Requesting evidence of internal audits would allow the client to review the vendor's commitment to maintaining and improving its internal procedures and security controls.

Option A is incorrect. While a business continuity plan is essential, it primarily outlines how disruptions will be managed and does not necessarily provide evidence of the vendor's internal control practices.

Option B is incorrect. Knowing the vendor's clients can provide some context, but it does not directly provide evidence of the vendor's internal control practices or security measures.

Option D is incorrect. The company's mission statement provides an overview of the company's goals and values but doesn't provide specific evidence of its internal control practices.

Question 510. GlobalFin, a fintech company, has developed a new mobile banking application. To avoid any legal complications, which of the following legal external considerations should GlobalFin pay the most attention to before launching the application worldwide?

- (A) **Ensuring the app meets global data privacy laws**
- (B) Confirming the color scheme aligns with branding regulations in all countries
- (C) Securing copyrights for all images used in the app
- (D) Making sure the app's name isn't offensive in any language

Explanation 510. Correct Answer: A. Ensuring the app meets global data privacy laws. For a mobile banking application, ensuring compliance with global data privacy laws is paramount. Different regions have varying requirements and regulations about how user data should be handled, stored, and processed.

Option B is incorrect. While branding and color schemes are important for marketing, they are not typically subjects of strict legal regulation like data privacy laws.

Option C is incorrect. While securing copyrights is important, the primary legal concern for a banking application would be related to data privacy and security, given the sensitive nature of financial data.

Option D is incorrect. Although it's good practice to ensure an app's name is culturally sensitive, the primary legal concern for a banking app would be data privacy and security regulations.

Question 511. MedTech, a medical device manufacturer, did not adhere to the required standards for device security and patient data protection. Which of the following repercussions might be the MOST critical for MedTech's ongoing operations?

- (A) Increased public relations campaigns
- (B) Short-term stock price fluctuations
- (C) Offering discounts on their devices
- (D) **Loss of license to manufacture and distribute**

Explanation 511. Correct Answer: D. Loss of license to manufacture and distribute. For a medical device manufacturer, maintaining adherence to industry-specific standards is crucial. Non-compliance, especially when it involves patient data protection, can lead to the company losing its license to operate.

Option A is incorrect. While public relations campaigns might be employed to manage reputation, it's not a direct consequence of non-compliance.

Option B is incorrect. Stock price fluctuations could occur due to many factors, but it's not the most critical consequence concerning the company's ability to operate.

Option C is incorrect. Offering discounts might be a strategy to regain customer trust, but it's not a direct result of non-compliance nor is it as critical as the potential loss of a license.

Question 512. Your organization has been repeatedly ignoring the security guidelines set forth by a global standards organization, despite having pledged adherence. Given the

repetitive nature of these violations, the organization is now facing disciplinary measures. Which of the following is the MOST likely immediate consequence of these actions?

- (A) Immediate revocation of business licenses
- (B) Sanctions imposed by the global standards organization**
- (C) Forcible shutdown of all online operations for a determined period
- (D) Mandatory public apology to stakeholders

Explanation 512. Correct Answer: B. Sanctions imposed by the global standards organization. Sanctions are penalties or other means of enforcement used to provide incentives for obedience with the law, or with rules and regulations. In this scenario, the global standards organization can impose sanctions for the failure to adhere to their guidelines.

Option A is incorrect. Revocation of business licenses is typically a drastic measure and might be taken by a local or national regulatory body, not a standards organization.

Option C is incorrect. While some sanctions might involve restrictions, forcibly shutting down all online operations would be an extreme and less likely measure for non-compliance with guidelines from a standards organization.

Option D is incorrect. A public apology, while potentially useful for public relations, is not a direct consequence or sanction imposed by most standards organizations.

Question 513. HealthCareNow, a large hospital chain, wants to ensure its newly implemented electronic health record (EHR) system adheres to national standards. Which type of audit would be most appropriate to confirm that HealthCareNow is in compliance with national regulations regarding patient data?

- (A) Self-assessment using internal standards
- (B) Third-party risk assessment
- (C) **External regulatory audit**
- (D) Informal peer review

Explanation 513. Correct Answer: C. External regulatory audit. External regulatory audits are conducted by external entities to ensure that organizations are complying with industry or national regulations. For HealthCareNow, an external regulatory audit will confirm that its EHR system complies with national standards related to patient data.

Option A is incorrect. While self-assessments are beneficial for internal reviews, they might not carry the same weight or depth of scrutiny that external regulatory audits possess.

Option B is incorrect. Third-party risk assessments focus on evaluating the security risks associated with external partners and vendors, not on confirming compliance with national regulations.

Option D is incorrect. An informal peer review might offer insights and suggestions but lacks the formal structure and regulatory emphasis of an external audit.

Question 514. In preparation for an upcoming audit, AlphaTech Corporation hires a team to evaluate their security measures. The team is spotted attempting to bypass security barriers, unlock doors without keys, and trying to access restricted floors by pretending to be maintenance staff. What type of testing is AlphaTech Corporation undergoing?

- (A) Network vulnerability scanning
- (B) **Physical penetration testing**
- (C) OS fingerprinting
- (D) Source code review

Explanation 514. Correct Answer: B. Physical penetration testing. Physical penetration testing involves hands-on techniques to breach physical barriers, such as locks, security checkpoints, or restricted areas, to assess the efficacy of physical security controls.

Option A is incorrect. Network vulnerability scanning is about identifying vulnerabilities in networked systems through automated tools, not physical barriers.

Option C is incorrect. OS fingerprinting identifies the operating system of a remote computer. It doesn't involve physically trying to access restricted areas.

Option D is incorrect. Source code review evaluates the source code of applications for vulnerabilities and doesn't concern physical access controls.

Question 515. Emily, a cybersecurity analyst, has been tasked with gathering preliminary information about a target

organization without directly interacting with its systems. She decides to collect data from third-party sources, search engines, public records, and other online platforms without sending any packets to the target. Which phase of penetration testing is Emily currently engaged in?

- (A) Active reconnaissance
- (B) **Passive reconnaissance**
- (C) Vulnerability scanning
- (D) Threat hunting

Explanation 515. Correct Answer: B. Passive reconnaissance. Passive reconnaissance is the initial phase in which the penetration tester collects information about the target without directly engaging with or alerting the target. Emily's approach of gathering data from third-party sources without sending packets or interacting directly with the target's systems is in line with the characteristics of passive reconnaissance.

Option A is incorrect. Active reconnaissance involves directly interacting with the target systems, often sending packets or probes, which can potentially be detected by the target.

Option C is incorrect. Vulnerability scanning is a step further where specific tools are used to identify vulnerabilities in a system. It is more direct than passive reconnaissance.

Option D is incorrect. Threat hunting is a proactive approach to finding malicious activities within a system rather than gathering information about a target system.

Question 516. As part of an initial penetration testing phase, Jackson is using tools that directly probe and interact with the target system's network to discover open ports, services, and other potential access points. While this approach is more direct and could be detected by the target's security systems, it provides detailed and actionable insights. Which type of reconnaissance is Jackson performing?

- (A) Threat analysis
- (B) Passive reconnaissance
- (C) **Active reconnaissance**
- (D) Social engineering

Explanation 516. Correct Answer: C. Active reconnaissance.

Active reconnaissance involves directly interacting with the target systems to gain more detailed and actionable information. In this phase, tools and techniques that can be detected by the target's security measures, such as port scanning, are often used. Jackson's approach matches the characteristics of active reconnaissance.

Option A is incorrect. Threat analysis is the process of identifying, assessing, and prioritizing threats against a system or organization.

Option B is incorrect. Passive reconnaissance is about collecting data without direct interaction with the target systems, typically using third-party sources, public records, and other non-intrusive methods.

Option D is incorrect. Social engineering involves manipulating individuals to reveal confidential information or

perform certain actions, and it is not directly related to network probing or service discovery.

Question 517. TechFirm, a leading technology conglomerate, recently conducted a security exercise. The goal was for the internal security team to defend against a series of simulated attacks from an external red team. While the red team launched attacks, the internal team's objective was to detect, respond, and mitigate those threats. What type of penetration testing is TechFirm employing for its internal security team?

- (A) Offensive penetration testing
- (B) Passive penetration testing
- (C) **Defensive penetration testing**
- (D) Black box testing

Explanation 517. Correct Answer: C. Defensive penetration testing. Defensive penetration testing is designed to test the organization's capability to defend its systems and networks against attacks. It typically involves an internal security team (often called the blue team) that defends against simulated attacks.

Option A is incorrect. Offensive penetration testing involves actively trying to exploit vulnerabilities, not defending against them.

Option B is incorrect. Passive penetration testing refers to gathering information without actively interacting with the target systems. It's not focused on defending against active threats.

Option D is incorrect. Black box testing is a method where the tester has no knowledge of the internal workings of the system they are testing. It doesn't describe a defensive posture.

Question 518. Emily, an executive assistant, receives a phone call from an individual claiming to be a new employee in the IT department. The caller says they're conducting a routine check and needs Emily to confirm her username and password for system verification. How should Emily respond?

- (A) Politely decline and report the call to the IT department**
- (B)** Provide the caller with the username but not the password
- (C)** Ask the caller to email the request, so there's a written record
- (D)** Hang up without saying anything

Explanation 518. Correct Answer: A. Politely decline and report the call to the IT department. This is a classic example of a vishing (voice phishing) attempt, a form of social engineering. The best practice in such scenarios is to never provide sensitive information over the phone, especially when the call is unsolicited. Reporting the attempt to the IT department can help the company be aware and potentially prevent further attempts.

Option B is incorrect. Even if Emily provides only her username, it could still be used maliciously in combination with other attacks.

Option C is incorrect. Written records can be helpful, but it's crucial not to entertain or validate unsolicited requests, whether via email or phone.

Option D is incorrect. While hanging up stops the immediate threat, it's essential to report such incidents for broader organizational awareness and protection.

Question 519. XYZ Corp, a manufacturer of smart home devices, failed to implement standard security practices in their products. A popular tech review site publishes an in-depth review detailing these vulnerabilities. Which of the following outcomes is XYZ Corp MOST likely to face as an immediate result?

- (A) An award for innovation in smart home technologies
- (B) **Reputational damage leading to decreased sales**
- (C) An increased partnership with tech retailers
- (D) A surge in the employee recruitment rate

Explanation 519. Correct Answer: B. Reputational damage leading to decreased sales. Negative reviews, especially those highlighting security vulnerabilities, can lead to a loss of trust among consumers, potentially resulting in decreased sales due to reputational damage.

Option A is incorrect. Receiving an award for innovation is unlikely in the face of publicized security vulnerabilities.

Option C is incorrect. Partnerships with tech retailers might be jeopardized, or at least put on hold, given the negative publicity around the product's security flaws.

Option D is incorrect. A negative review, especially one that underscores security vulnerabilities, is unlikely to boost recruitment. Potential employees may be wary of joining a company with a tarnished reputation.

Question 520. SoftTech Inc., a software company, is considering expanding its operations to Europe. They will be collecting and processing personal data of EU citizens. Which of the following legal implications is MOST critical for SoftTech Inc. to consider?

- (A) The need to register with each country's software association
- (B) Compliance with the General Data Protection Regulation (GDPR)**
- (C) Ensuring software patent rights in each European country
- (D) The European standard for software coding

Explanation 520. Correct Answer: B. Compliance with the General Data Protection Regulation (GDPR). When dealing with personal data of EU citizens, companies must comply with the GDPR, which outlines strict requirements on data protection and privacy. Non-compliance can lead to hefty fines and legal repercussions.

Option A is incorrect. Registering with each country's software association is not related to the privacy and legal implications of processing personal data.

Option C is incorrect. While software patent rights are essential, they don't directly address the privacy concerns of processing personal data of EU citizens.

Option D is incorrect. There is no "European standard for software coding" that relates to the privacy of personal data. The critical concern is data protection and privacy regulations like the GDPR.

Question 521. DataGuard Corp. operates in the European Union and has recently suffered a major data breach affecting the personal data of thousands of users. They failed to comply with some key provisions of the General Data Protection Regulation (GDPR). Which of the following is the MOST likely immediate consequence of their non-compliance?

- (A) They will be forced to shut down operations until compliance is achieved
- (B) DataGuard's executive team will face immediate imprisonment
- (C) The company will be required to issue a public apology
- (D) **DataGuard Corp. will face substantial fines for their non-compliance**

Explanation 521. Correct Answer: D. DataGuard Corp. will face substantial fines for their non-compliance. The GDPR provisions can levy hefty fines on organizations that do not comply with its requirements, especially in the case of data breaches. The fines can be up to 4% of the annual global turnover or €20 million, whichever is higher.

Option A is incorrect. While the GDPR can impose operational restrictions, it does not directly mandate shutdowns of companies due to non-compliance.

Option B is incorrect. GDPR does not call for the imprisonment of executive teams. However, non-compliance can lead to severe fines.

Option C is incorrect. While issuing a public apology might be a good PR move, it is not a direct consequence enforced by GDPR.

Question 522. SafeNet, a financial institution, decided to undertake a comprehensive security assessment. They brought together their internal security team and an external group of ethical hackers. Their objective was for these teams to collaboratively assess vulnerabilities, perform real-time attack simulations, and evaluate defense mechanisms. What form of penetration testing is SafeNet utilizing?

- (A) Black box testing
- (B) **Integrated penetration testing**
- (C) Defensive penetration testing
- (D) Red team assessment

Explanation 522. Correct Answer: B. Integrated penetration testing. Integrated penetration testing, often associated with purple teaming, involves the combined efforts of both offensive and defensive teams to provide a holistic assessment of an organization's security posture.

Option A is incorrect. Black box testing is a method where the tester doesn't have prior knowledge of the system's architecture or underlying code. It doesn't emphasize the collaborative nature between offensive and defensive teams.

Option C is incorrect. Defensive penetration testing focuses on evaluating the defensive capabilities of an organization against potential attacks, without necessarily implying collaboration with an offensive team.

Option D is incorrect. Red team assessment involves simulating real-world cyber-attacks to test an organization's security posture, but it doesn't inherently suggest a joint effort with a defensive team.

Question 523. AlphaTech, a leading tech manufacturer, is considering a penetration test to identify vulnerabilities in their new product's firmware. They provide the testers with firmware source code, architecture diagrams, and other internal details to ensure a thorough evaluation. What kind of penetration test is AlphaTech commissioning?

- (A) Zero-knowledge testing
- (B) **Open box testing**
- (C) Opaque testing
- (D) Blind testing

Explanation 523. Correct Answer: B. Open box testing.

Open box testing, similar to white box testing, is where the tester is given complete transparency and full details about the system internals, making it easier to identify vulnerabilities that might be missed in other forms of testing.

Option A is incorrect. Zero-knowledge testing is another term for black box testing, where testers have no knowledge of the system internals.

Option C is incorrect. Opaque testing is not a recognized term in penetration testing methodologies and is intended as a distractor.

Option D is incorrect. Blind testing is a scenario where the testers have limited knowledge about the target system.

Question 524. John, a citizen of a country that strictly follows the General Data Protection Regulation (GDPR), used a global online shopping platform for a year. He decided to stop using the platform and requested the deletion of all his personal data. What is the online platform's primary obligation concerning John's request under the "Right to be Forgotten" principle?

- (A) Retain the data but ensure that John's data is never used for marketing purposes
- (B) Delete all personal data about John unless there's a legal reason to keep it**
- (C) Anonymize John's data and notify him of the completion
- (D) Move John's data to a secure, encrypted server where it won't be accessed

Explanation 524. Correct Answer: B. Delete all personal data about John unless there's a legal reason to keep it. The "Right to be Forgotten" under GDPR allows citizens to ask organizations to delete their personal data unless the

organization has a legitimate reason (e.g., legal obligations) to retain the data.

Option A is incorrect. Merely refraining from using John’s data for marketing does not satisfy the “Right to be Forgotten.”

Option C is incorrect. Anonymization does not equate to the removal of data, and GDPR’s “Right to be Forgotten” specifically refers to the deletion of data.

Option D is incorrect. Simply moving the data to a secure server doesn’t align with the principles of the “Right to be Forgotten.” The data needs to be deleted unless there’s a valid reason to retain it.

Question 525. WebMasters LLC, a popular web hosting company, wants to ensure the robust security of their hosted websites. They initiate a security challenge, inviting ethical hackers worldwide to find vulnerabilities without giving any details about their servers, databases, or applications. Which penetration testing method is WebMasters LLC utilizing?

- (A) External testing
- (B) Grey box testing
- (C) Active testing
- (D) **Black box testing**

Explanation 525. Correct Answer: D. Black box testing. In black box testing, the testers are not provided with any knowledge about the system’s internals and have to identify vulnerabilities based purely on their own discoveries.

WebMasters LLC's approach, where they don't disclose any specifics to the ethical hackers, resonates with this method.

Option A is incorrect. While the challenge by WebMasters LLC can be externally focused, external testing alone doesn't define the level of knowledge provided to the testers.

Option B is incorrect. In grey box testing, testers would have some knowledge about the target, which is not the case here.

Option C is incorrect. Active testing simply means testers are directly interacting with the system, but it doesn't specify the amount of knowledge they have about its internals.

Question 526. After a series of high-profile data breaches in the industry, OnlineRetail Corp., an e-commerce platform, wishes to undergo an external review to validate the security of its operations and provide a comprehensive report to its shareholders. Which type of assessment will provide a detailed and formalized examination of their security posture?

- (A) **External examination of IT controls and operations**
- (B) Internal review of security protocols
- (C) External regulatory audit on financial statements
- (D) Informal feedback from industry peers

Explanation 526. Correct Answer: A. External examination of IT controls and operations. An external examination of IT controls and operations provides a deep and structured assessment of an organization's security posture and IT operations. Conducted by external experts, it can provide

formalized, comprehensive findings to reassure shareholders of the company's security measures.

Option B is incorrect. An internal review is conducted by the organization's own personnel and may lack the independent perspective and comprehensive scope of an external examination.

Option C is incorrect. An external regulatory audit on financial statements focuses on financial reporting and not on the security of IT operations.

Option D is incorrect. Informal feedback, while potentially useful, does not offer the structured, comprehensive, and independent insights that an external examination provides.

Question 527. WebFirm, a web development company, did not comply with the data handling and protection clauses outlined in their contract with RetailMax, an e-commerce company. As a result, RetailMax's customer data was exposed in a data breach. Which of the following is the MOST probable contractual impact on WebFirm due to this incident?

- (A) WebFirm will receive bonuses for early project completion
- (B) WebFirm will be required to provide additional services at no cost
- (C) **RetailMax will terminate the contract and may seek damages**
- (D) RetailMax will extend the project timeline

Explanation 527. Correct Answer: C. RetailMax will terminate the contract and may seek damages. A data breach, especially one that results from non-compliance with contractual clauses related to data protection, can lead to the termination of the contract. Additionally, the affected party, in this case, RetailMax, might also seek damages from WebFirm for the breach.

Option A is incorrect. Bonuses for early project completion are unrelated to non-compliance with data protection clauses.

Option B is incorrect. While some contracts might stipulate penalties such as providing additional services for breaches, in a significant incident like a data breach, termination is more probable.

Option D is incorrect. Extending the project timeline is not a typical response to a breach of data protection clauses in a contract.

Question 528. SafeNet Banking Corporation is keen on gaining a competitive edge in the market by demonstrating its commitment to cybersecurity. They want an official attestation that their cybersecurity measures are robust and compliant with industry standards. What should SafeNet opt for to obtain this attestation?

- (A) Feedback from customers on the bank's app security
- (B) Internal IT team's report on cybersecurity practices
- (C) **External independent third-party audit**
- (D) Informal evaluation by a cybersecurity consultancy

Explanation 528. Correct Answer: C. External independent third-party audit. An external independent third-party audit can provide an official attestation regarding SafeNet Banking Corporation's adherence to industry standards in cybersecurity. By having an external entity evaluate their practices, SafeNet can assure stakeholders of its commitment to cybersecurity.

Option A is incorrect. While feedback from customers is valuable, it is not an official or comprehensive assessment of the bank's entire cybersecurity practices.

Option B is incorrect. An internal IT team's report might lack the external perspective and official attestation that a third-party audit can provide.

Option D is incorrect. An informal evaluation, even by a cybersecurity consultancy, might not be as rigorous or recognized as an official third-party audit.

Question 529. XYZ Corp., a multinational company, recently underwent a security audit. The Chief Information Security Officer (CISO) needs to report the findings of the audit to the company's internal stakeholders as well as to a governmental regulatory agency. Which of the following represents the correct type of compliance reporting for each recipient?

- (A) Internal report for the regulatory agency and external report for internal stakeholders
- (B) External report for both the regulatory agency and internal stakeholders
- (C) **Internal report for internal stakeholders and external report for the regulatory agency**

(D) No report is required for internal stakeholders, only an external report for the regulatory agency

Explanation 529. Correct Answer: C. Internal report for internal stakeholders and external report for the regulatory agency. Internal compliance reports are typically designed for consumption within the organization and may contain details that are not shared externally. External compliance reports, on the other hand, are designed for entities outside of the organization, such as regulators or other third parties, and would contain information that is relevant and necessary for those entities to review.

Option A is incorrect. It is not standard to provide an internal report for an external entity or an external report for internal stakeholders.

Option B is incorrect. While it's conceivable to use the same report for both internal and external entities, it's more common to tailor reports to the specific audience. An internal report may contain more detailed or sensitive information not suitable for an external audience.

Option D is incorrect. It is crucial for internal stakeholders to be aware of the audit findings to make informed decisions and plan remediation actions.

Question 530. SoftTech Solutions is a software development company that has decided to conduct a penetration test on their new web application. The testers are provided with user credentials, network topology diagrams, and some proprietary

software code snippets. Which type of penetration testing is SoftTech Solutions employing?

- (A) Black box testing
- (B) Double-blind testing
- (C) **Known environment testing**
- (D) Zero-knowledge testing

Explanation 530. Correct Answer: C. Known environment testing. Known environment testing is a type of penetration testing where the testers are given certain information about the target's environment. This can include user credentials, network diagrams, and more, to mimic a potential insider threat or a threat actor who has gained certain internal information.

Option A is incorrect. In black box testing, testers are given no prior knowledge about the system.

Option B is incorrect. In double-blind testing, neither the attackers nor the defenders have prior knowledge of the impending test.

Option D is incorrect. Zero-knowledge testing is another term for black box testing, where the testers have no knowledge of the system internals.

Question 531. A medium-sized organization recently had a third-party auditor review their information security controls. After the review, the auditor provided a formal statement that verified the effectiveness of the controls in place. What is this formal statement referred to as?

- (A) Certification

- (B) Accreditation
- (C) **Attestation**
- (D) Assurance

Explanation 531. Correct Answer: C. Attestation. An attestation is a formal statement or declaration by a subject matter expert, like an auditor, attesting that specific criteria are met. In this case, the auditor is attesting to the effectiveness of the information security controls.

Option A is incorrect. Certification is the process of providing someone or something with an official document attesting to a status or level of achievement, which may or may not involve testing against certain standards.

Option B is incorrect. Accreditation is the formal recognition that a body or individual is competent to perform specific tasks, usually granted by a higher authority or body.

Option D is incorrect. Assurance refers to the measures taken to gain confidence in the security of a system, but it's not a formal declaration like an attestation.

Question 532. CyberLock Inc. is assessing the security postures of its third-party vendors to determine potential risks. The cybersecurity team wants to gather foundational security information from each vendor to evaluate their security maturity and practices. What would be the most cost-effective and efficient way to collect this data from a large number of vendors?

- (A) Conduct a penetration test for each vendor

- (B) Send out security questionnaires to each vendor
- (C) Visit each vendor's site for an in-person assessment
- (D) Review the annual financial reports of each vendor

Explanation 532. Correct Answer: B. Send out security questionnaires to each vendor. Security questionnaires are commonly used to gather foundational security information from third-party vendors. They are cost-effective and can efficiently collect standardized data from a large number of vendors to evaluate their security posture and practices.

Option A is incorrect. Conducting a penetration test for each vendor would be resource-intensive, costly, and may not provide the foundational information about the vendor's security practices.

Option C is incorrect. Visiting each vendor's site for an in-person assessment would be time-consuming, costly, and logistically challenging, especially when dealing with a large number of vendors.

Option D is incorrect. Annual financial reports provide financial data and do not offer in-depth details on a vendor's security posture or practices.

Question 533. TechGuard Inc. and CloudSecure are two cybersecurity firms that are considering a collaboration on a new cloud security project. Both companies have proprietary technologies and methodologies they will bring into the partnership. Before embarking on the collaborative venture, which agreement should they finalize to define the terms of

their partnership, roles, and shared responsibilities?

- (A) Non-disclosure agreement (NDA)
- (B) Service-level agreement (SLA)
- (C) **Business partners agreement (BPA)**
- (D) Memorandum of understanding (MOU)

Explanation 533. Correct Answer: C. Business partners agreement (BPA). A Business partners agreement (BPA) outlines the specifics of the partnership between entities, detailing roles, responsibilities, financial arrangements, and other key terms of the relationship. Given that TechGuard Inc. and CloudSecure are forming a partnership with shared roles and responsibilities, a BPA is the most fitting.

Option A is incorrect. An NDA focuses specifically on the confidentiality of shared information and not on the broader terms of a partnership.

Option B is incorrect. A service-level agreement (SLA) centers on the standards and quality of service to be provided, detailing performance metrics, and does not focus on partnership specifics.

Option D is incorrect. An MOU signifies mutual intentions and understanding between parties but may not provide detailed terms and conditions of a business partnership like a BPA does.

Question 534. XYZ Ltd. wants to evaluate if their current security measures are consistent with industry-specific regulations they are required to follow. The evaluation should be done by their own IT department before inviting external

auditors. Which approach should XYZ Ltd. adopt?

- (A) Third-party vulnerability scanning
- (B) **Internal compliance assessment**
- (C) External attestation
- (D) Vendor risk assessment

Explanation 534. Correct Answer: B. Internal compliance assessment. An internal compliance assessment is conducted by an organization's internal teams to evaluate if their operations, processes, and configurations are in alignment with required compliance standards or regulations. This helps in proactively identifying and rectifying non-compliance before an external audit.

Option A is incorrect. Third-party vulnerability scanning focuses on identifying vulnerabilities and doesn't necessarily check for compliance with industry-specific regulations.

Option C is incorrect. External attestation is a formal statement from an external party verifying specific criteria. This would not be done by the company's internal IT department.

Option D is incorrect. Vendor risk assessment focuses on assessing the security risks associated with third-party vendors and doesn't evaluate an organization's internal compliance with regulations.

Question 535. A cybersecurity firm has been hired by TechGiant Corp. to perform penetration testing on their infrastructure. Before the testing begins, the CEO of TechGiant Corp. wants to ensure that certain critical systems are not

targeted, and that the testing will not disrupt their ongoing operations. What should be established to define the scope and boundaries of the test?

- (A) Service-level agreement (SLA)
- (B) Non-disclosure agreement (NDA)
- (C) **Rules of engagement (ROE)**
- (D) Memorandum of understanding (MOU)

Explanation 535. Correct Answer: C. Rules of engagement (ROE). The Rules of Engagement (ROE) document defines the scope, boundaries, methods, and other critical guidelines for a penetration test. It ensures that both the testing team and the organization understand and agree on what can and cannot be done during the testing.

Option A is incorrect. A Service-level agreement (SLA) primarily deals with the levels of service expected, such as uptime, response times, etc. It doesn't define the boundaries of a penetration test.

Option B is incorrect. A Non-disclosure agreement (NDA) is about keeping information confidential and wouldn't define the scope of a penetration test.

Option D is incorrect. A Memorandum of understanding (MOU) is a general agreement between parties, but it doesn't detail the specific scope and rules of a penetration test like the ROE would.

Question 536. As part of the annual security training, the IT department of XYZ Corp decides to launch a simulated

phishing campaign. The aim is to assess employees' ability to identify and report phishing emails. Which of the following would be the MOST effective first step in ensuring the success of this campaign?

- (A) Informing all employees about the campaign a week prior
- (B) **Creating a realistic phishing email that closely resembles common threats**
- (C) Offering rewards to employees who click on the simulated phishing links
- (D) Reviewing the results of the previous year's campaign

Explanation 536. Correct Answer: B. Creating a realistic phishing email that closely resembles common threats. For the phishing campaign to effectively assess employees' ability to recognize phishing threats, the simulated phishing email must be as realistic as possible. By making it closely resemble common threats, the IT department can gain a more accurate measure of the employees' awareness and response.

Option A is incorrect. Informing all employees about the campaign beforehand would defeat the purpose of the test, as they would be expecting a phishing email and thus be more likely to recognize and report it.

Option C is incorrect. Offering rewards to employees who click on the simulated phishing links would encourage risky behavior and is counterproductive to the goal of increasing security awareness.

Option D is incorrect. While reviewing results from previous campaigns can provide insights, it would not be the most effective first step in ensuring the success of the current campaign.

Question 537. A healthcare provider wants to evaluate the security of their patient portal. They inform the penetration testers about the technologies used, such as the programming languages and databases. However, specifics about the security measures in place, including intrusion detection systems, are kept secret. What kind of penetration test are they aiming for?

- (A) White box testing
- (B) External testing
- (C) **Grey box testing**
- (D) Active testing

Explanation 537. Correct Answer: C. Grey box testing. Grey box testing implies that testers have some knowledge about the target but not all details. Here, the healthcare provider gives details about the technologies used but keeps information about the security measures a secret. This partial disclosure aligns with grey box testing methodology.

Option A is incorrect. In white box testing, testers would have a complete overview of the system, including its code, configurations, and security measures.

Option B is incorrect. External testing primarily focuses on the system's exterior defenses, like firewall configurations, without consideration of what details are shared with the testers.

Option D is incorrect. Active testing means testers are directly interacting with the system and is not indicative of the level of knowledge they possess about the system's internals.

Question 538. TechFirm Inc. collects personal data from its users and decides on the purposes and means of processing this data. They also outsource data storage to CloudData, a third-party company. In the context of data privacy regulations, how would TechFirm and CloudData be classified respectively?

- (A) TechFirm: Processor; CloudData: Controller
- (B) **TechFirm: Controller; CloudData: Processor**
- (C) Both TechFirm and CloudData: Processors
- (D) Both TechFirm and CloudData: Controllers

Explanation 538. Correct Answer: B. TechFirm: Controller; CloudData: Processor. TechFirm Inc., which decides on the purposes and means of processing personal data, is the “Controller”. CloudData, which is responsible for processing data on behalf of TechFirm (without deciding on its use), is the “Processor”.

Option A is incorrect. The roles are reversed in this option. TechFirm is the one making decisions on data use, so it's the Controller.

Option C is incorrect. Both entities have different roles in this scenario. TechFirm is not just processing; it's deciding on how the data should be used, making it a Controller.

Option D is incorrect. CloudData does not decide on the purpose and means of the data processing. It simply processes data on behalf of TechFirm, making it a Processor.

Question 539. Sarah, a sales manager at TechWorld Inc., receives an email from her bank urging her to update her account details due to a recent security breach. The email provides a link to a website that looks almost identical to her bank's official site. However, she notices a slight misspelling in the URL. What should Sarah do next?

- (A) Forward the email to her colleagues as a warning
- (B) Click the link and update her details as the bank's site is probably just undergoing updates
- (C) Delete the email without taking any action
- (D) Report the email to her company's IT department and avoid clicking any links**

Explanation 539. Correct Answer: D. Report the email to her company's IT department and avoid clicking any links.

Sarah likely received a phishing email, a common tactic used by attackers to deceive users into providing sensitive information. The best course of action is to report the suspicious email to the IT department so they can take necessary precautions and notify other employees.

Option A is incorrect. While Sarah has the right instinct to warn others, forwarding potentially malicious emails can lead to more risks. It's better to alert the IT department.

Option B is incorrect. Clicking on links in suspicious emails, especially with a misspelled URL, can lead to compromised personal and company data.

Option C is incorrect. Simply deleting the email doesn't address the broader risk to the organization. Reporting such incidents helps the company bolster its defenses.

Question 540. WebSoft Inc., a leading software company, recently launched a new web application. Before making it live, they engaged a security firm to challenge the application, find vulnerabilities, and exploit them as real hackers would. This aggressive testing is done to ensure maximum security. What kind of penetration testing is WebSoft Inc. opting for?

- (A) White box testing
- (B) Defensive penetration testing
- (C) **Offensive penetration testing**
- (D) Gray box testing

Explanation 540. Correct Answer: C. Offensive penetration testing. Offensive penetration testing is an aggressive form of testing where the tester actively attempts to find and exploit vulnerabilities in the target system or application, much like a real attacker.

Option A is incorrect. White box testing, also known as clear box testing, involves having full visibility and knowledge of the internal workings of the application being tested. The focus is more on the methodology and not the aggressive nature of the testing.

Option B is incorrect. There is no specific testing method called “defensive penetration testing.” Defensive strategies are typically associated with blue team activities that focus on defending systems, not aggressively testing them.

Option D is incorrect. Gray box testing is a combination of both white box and black box testing methods. Testers have some knowledge of the internal workings but not complete information. The emphasis here is on the level of knowledge of the system and not on the aggressive nature of the testing.

EXAM SIMULATOR #1

Questions 1-100

Question 1. A smart city project is deploying various IoT sensors across the city to gather data on traffic patterns, weather, pollution levels, and more. Which of the following is the MOST critical security consideration when deploying these sensors?

- (A) Ensuring high data transfer speeds to cater to the volume of data from the IoT sensors
- (B) Limiting the IoT devices to communicate only with specific, pre-defined servers
- (C) Installing physical locks on IoT devices to prevent theft
- (D) Allowing IoT devices to connect to any available network for data redundancy

Question 2. TechFirm Inc. has decided to engage in a new business venture. Before they move forward, the security team conducts several brainstorming sessions, interviews, and reviews historical data to generate a list of potential security threats that the new venture could face. This activity is a primary component of which step in the risk management process?

- (A) Risk assessment
- (B) Risk response
- (C) Risk monitoring
- (D) Risk identification

Question 3. A large financial organization wants to ensure that all employees understand the importance of cybersecurity and the role they play in safeguarding company assets. Which of the following managerial security controls will be MOST effective in achieving this?

- (A) Installing a firewall at the network perimeter
- (B) Regular security awareness training for employees
- (C) Deploying an Intrusion Detection System (IDS)
- (D) Encrypting all company data

Question 4. A major pharmaceutical company recently announced an increase in drug prices. Following the announcement, their website was taken offline by a DDoS attack, with a message posted online by a group claiming responsibility and demanding affordable healthcare for all. Which type of threat actor is MOST likely behind this attack?

- (A) Unskilled attacker
- (B) Insider threat
- (C) Hacktivist
- (D) Nation-state

Question 5. After deploying wireless access points in a large manufacturing facility, employees report inconsistent wireless connectivity in some areas. What tool would be most effective for the IT team to use to visualize areas of weak wireless signal strength?

- (A) Network bandwidth monitor
- (B) Protocol analyzer
- (C) Heat map software
- (D) Intrusion detection system

Question 6. In an IaaS (Infrastructure as a Service) model, which of the following tasks is typically the responsibility of the cloud customer in a standard Cloud Responsibility Matrix?

- (A) Physical security of data centers
- (B) Patching of host operating systems
- (C) Network infrastructure maintenance
- (D) Patching of guest operating systems

Question 7. A company's website was temporarily defaced with a humorous meme, but no sensitive data was stolen or any significant damage done. The attacker left a message bragging about their first successful hack. Which type of threat actor is MOST likely responsible for this attack?

- (A) Insider threat
- (B) Advanced Persistent Threat (APT)
- (C) Unskilled attacker
- (D) Nation-state

Question 8. A financial institution recently discovered that a large number of confidential customer records were being accessed and copied during off-business hours. Upon investigation, it was found that the access came from an authenticated user within the company, who had recently been passed over for a promotion. Which type of threat actor is MOST likely responsible for this security incident?

- (A) Hacktivist
- (B) Insider threat
- (C) Nation-state
- (D) Organized crime syndicate

Question 9. A company is evaluating its data storage options. They need a solution that provides them with the highest level of control over their hardware, software, and network configurations, allowing for customized security controls and measures. Which deployment model would best suit their needs?

- (A) Cloud-based Infrastructure
- (B) Hybrid Infrastructure
- (C) On-premises Infrastructure
- (D) Community Cloud

Question 10. A new technology firm recently launched a device that uses facial recognition for authentication. A cybersecurity researcher, without any malicious intent, demonstrated a method to bypass the facial recognition using a photograph. The researcher then approached the firm with the findings without publicizing it. What is the primary motivation behind the researcher's action?

- (A) Philosophical beliefs opposing facial recognition
- (B) Financial gain by blackmailing the firm
- (C) Ethical considerations for consumer security
- (D) Aiming to damage the firm's market reputation

Question 11. ABC Corp recently adopted a Bring Your Own Device (BYOD) policy. The IT department is concerned about the potential risks associated with personal devices accessing the corporate network. Which of the following solutions would be MOST effective for enforcing security policies on these personal mobile devices?

- (A) Installing antivirus software on each device
- (B) Establishing a separate guest Wi-Fi network for mobile

devices

- (C) Using Mobile Device Management (MDM) to enforce security policies
- (D) Mandating that employees use strong passwords on their personal devices

Question 12. AcmeTech, a software development firm, recently experienced a major data breach that was traced back to a vulnerability in their custom-built application. Post-incident analysis revealed that the vulnerability had been introduced during the coding phase and was never detected during testing. To avoid such vulnerabilities in the future, which policy should AcmeTech emphasize to ensure secure practices are maintained throughout the development process?

- (A) Incident Response Policy
- (B) Change Management Policy
- (C) Business Continuity Policy
- (D) Software Development Lifecycle (SDLC) Policy

Question 13. A high-profile executive received an email containing personal photos and a message threatening to release the images to the public unless a significant sum of money was transferred to a specific cryptocurrency address. What motivation is most evident behind this threat?

- (A) Espionage to gather competitive intelligence
- (B) Service disruption to harm the reputation of the executive's company
- (C) Blackmail to extract money by leveraging sensitive information
- (D) Data exfiltration for selling on the dark web

Question 14. A software development team in a large corporation decided to use an unauthorized cloud-based tool to host and manage their source code. The team believed it would increase their productivity, even though it was not approved by the IT department. A few weeks later, unauthorized access to their project data was detected. Which threat actor concept BEST describes the situation?

- (A) Insider threat
- (B) Hacktivist
- (C) Shadow IT
- (D) Organized crime syndicate

Question 15. A financial institution has experienced an uptick in unauthorized transactions. They want to implement a control that will allow them to identify suspicious transactions in real-time. Which of the following would be the BEST detective control for this scenario?

- (A) Implementing a multi-factor authentication system for all users
- (B) Establishing a Security Operations Center (SOC) to monitor network traffic
- (C) Installing an Intrusion Detection System (IDS) on their network
- (D) Restricting transaction capabilities to only a few trusted IP addresses.

Question 16. MegaTech Inc. is in the process of outlining a strategy to ensure that after any disaster, critical applications can be restored to a working state within 4 hours. The organization also wants to make sure that the data loss does not exceed 1 hour. Which of the following policies is most relevant

to achieving this objective?

- (A) Data Retention Policy
- (B) Incident Response Policy
- (C) Disaster Recovery Policy
- (D) Password Policy

Question 17. A large financial institution is planning to upgrade its IT infrastructure to allow for a more efficient use of hardware resources, faster deployment of applications, and reduced server provisioning times. While evaluating different technologies, which of the following would directly address these needs?

- (A) Network Segmentation
- (B) Intrusion Detection System
- (C) Virtualization
- (D) Multi-Factor Authentication

Question 18. Bob receives an email prompting him to verify his identity by clicking on a link. The link directs him to a webpage where he has to provide his username, password, and answer a personal security question. What type of authentication method is being employed here?

- (A) Biometric authentication
- (B) Token-based authentication
- (C) Two-factor authentication
- (D) Single sign-on

Question 19. An online banking website employs a system that automatically logs out users after 10 minutes of inactivity to ensure that if a user forgets to log out, no one else can alter the user's banking details. Which principle of the CIA triad is the

banking website MOST directly addressing?

- (A) Confidentiality
- (B) Availability
- (C) Authentication
- (D) Integrity

Question 20. A software development company is looking to migrate its legacy applications to a more modern infrastructure. They want to ensure the applications can be deployed consistently across multiple environments without the challenges of varying dependencies and configurations. Which approach would best achieve this goal?

- (A) Virtual Machine Deployment
- (B) Bare-Metal Deployment
- (C) Containerization
- (D) Serverless Computing

Question 21. Your organization is implementing Infrastructure as Code (IaC) to deploy and manage its cloud infrastructure. As part of a security review, what is a primary concern regarding the use of IaC scripts?

- (A) Lack of graphical interface for infrastructure visualization
- (B) Hardcoding sensitive data within the scripts
- (C) Inability to scale the infrastructure dynamically
- (D) Incompatibility with non-cloud environments

Question 22. A pharmaceutical company is concerned about competitors accessing their formula for a new drug. Which pillar of the CIA triad is MOST directly addressed by their concern?

- (A) Availability
- (B) Confidentiality
- (C) Integrity
- (D) Non-repudiation

Question 23. An online gaming platform experiences latency issues during multiplayer sessions, affecting the gameplay experience of its users. The company wants to ensure real-time responsiveness for its players worldwide. Which of the following solutions would BEST mitigate these latency issues?

- (A) Implementing a Content Delivery Network (CDN)
- (B) Introducing stricter user authentication methods
- (C) Deploying a centralized database server
- (D) Reducing the game's graphical fidelity

Question 24. A startup company anticipates rapid growth in its user base over the next year. They are considering an architectural model for their application that can handle the projected growth without performance issues. Which of the following would be the BEST design consideration for this situation?

- (A) Implementing strict password policies
- (B) Using a monolithic application design
- (C) Integrating a DDoS protection mechanism
- (D) Adopting a microservices architecture

Question 25. MedGuard, a health tech company, has developed an AI-driven software that predicts potential health risks based on patient data. Before launching in the U.S. market, which of the following industry external considerations should be the company's primary focus?

- (A) Integrating with popular fitness tracking apps in the U.S.
- (B) Ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA)
- (C) Surveying U.S. doctors about software interface preferences
- (D) Collaborating with U.S. pharmaceutical companies for promotional deals

Question 26. An e-commerce company has experienced a Distributed Denial of Service (DDoS) attack, which caused its website to become inaccessible for several hours. To mitigate the impact of such attacks in the future, which of the following would be the BEST corrective control to implement?

- (A) Displaying a seal for third-party security certifications on the website
- (B) Establishing a Web Application Firewall (WAF) with DDoS protection
- (C) Conducting routine vulnerability assessments on the website
- (D) Implementing strong password policies for website administrators

Question 27. A healthcare organization uses embedded systems in various medical devices. They are aware of the potential threats these systems can pose if not properly secured. Which of the following is NOT a recommended practice when hardening embedded systems in this context?

- (A) Regularly patching and updating the firmware of the devices
- (B) Allowing unrestricted access to the devices for ease of

use by the medical staff

(C) Disabling unnecessary services and features not required for the device's primary function

(D) Changing default credentials and using strong, unique passwords for device access

Question 28. A financial institution wants to ensure that customers are aware of the bank's policies on information sharing and how their personal data is used. Which of the following security controls would BEST communicate this to customers?

(A) Implementing end-to-end encryption for online transactions

(B) Publishing a privacy policy on the bank's website

(C) Conducting annual cybersecurity awareness training for employees

(D) Using multi-factor authentication for online banking

Question 29. A company detected a DDoS attack that lasted for several weeks. The attackers used a botnet of millions of infected devices and frequently rotated attack vectors to bypass mitigation efforts. This prolonged and resource-intensive attack suggests which kind of threat actor's resources and funding?

(A) Amateur hacker with minimal resources

(B) Cybersecurity researcher testing vulnerabilities

(C) Nation-state actor with strategic interests

(D) Organized crime syndicate with substantial funding

Question 30. AlphaCorp is migrating to cloud infrastructure and wants to ensure all virtual machines (VMs) are securely configured from the onset. Before deploying multiple VM

instances, what should AlphaCorp do to ensure each VM starts from a secure configuration?

- (A) Use the default VM templates provided by the cloud provider
- (B) Establish a secure baseline for VM configurations and use it for deployment
- (C) Regularly backup all VMs
- (D) Use multi-factor authentication for cloud access

Question 31. SecureNet Ltd. wants to protect user accounts from brute force attacks. They want to implement a measure where, after a certain number of failed login attempts, the account would become temporarily inaccessible. Which standard best suits this requirement?

- (A) Password minimum length
- (B) Account lockout threshold
- (C) Mandatory password resets
- (D) Two-factor authentication

Question 32. An energy company is looking to enhance the security of its ICS/SCADA systems. They have realized that default configurations might have vulnerabilities. Which of the following is the BEST initial step to take in securing their ICS/SCADA systems?

- (A) Connect the ICS/SCADA systems to the internet for remote monitoring
- (B) Use commercial off-the-shelf software to add a layer of security
- (C) Implement a secure baseline configuration tailored to the ICS/SCADA environment

(D) Increase the number of users with administrative privileges to ensure rapid response to issues

Question 33. The IT department wants to monitor network traffic in real time to detect any anomalies or malicious activities. Which of the following security controls can accomplish this?

- (A) Security policy documentation
- (B) Intrusion Detection System (IDS)
- (C) Employee code of conduct
- (D) Access Control Lists (ACL)

Question 34. A company is located in an area prone to natural disasters such as earthquakes and floods. Which of the following physical security controls would be MOST effective in ensuring the safety of the company's IT infrastructure?

- (A) Using biometric authentication for server access
- (B) Deploying a firewall to protect against cyber threats
- (C) Establishing a raised floor system in the data center
- (D) Conducting penetration testing on a regular basis

Question 35. A network engineer is preparing a new batch of routers for deployment in a large organization. Which of the following steps should the engineer prioritize to ensure that the routers are securely configured from the start?

- (A) Configure the routers to use DHCP to dynamically assign IP addresses to connected devices
- (B) Change the default administrative credentials on the routers
- (C) Update the routers' firmware to the latest, most feature-rich version, regardless of its security posture

(D) Customize the routers' LED colors for easy identification in the server room

Question 36. SecureCom, a telecommunications company, is planning to expand its infrastructure across Country A. The nation recently updated its telecommunications regulations and mandates strict guidelines for all external communications. Which of the following should be SecureCom's primary focus as it begins its expansion?

(A) Increasing advertising budget to gain a stronger market presence in Country A

(B) Ensuring its infrastructure meets the national standards for secure and encrypted communications

(C) Collaborating with local tech companies to better understand the culture of Country A

(D) Launching new products tailored to the preferences of Country A's residents

Question 37. A medical company has recently deployed a device to monitor patient heart rates in real time. This device uses a real-time operating system (RTOS) to guarantee immediate response times. The security team is concerned about potential risks. Which of the following would be a KEY recommendation to enhance the security of such devices?

(A) Ensure real-time data analysis capabilities

(B) Integrate the device with the corporate cloud for backups

(C) Implement strict network segmentation for the device

(D) Increase the storage capacity of the device

Question 38. DigitalZone Corp, a marketing company, collects personal data from users and determines how and why that data will be processed. At the same time, they engage an external company, CloudSolutions, to store and manage this data. In this scenario, what role does DigitalZone Corp play in relation to data protection regulations?

- (A) Processor
- (B) Data subject
- (C) Controller
- (D) Third-party provider

Question 39. During an annual review, a company discovered that one of its critical systems had several unscheduled downtimes over the year. The CTO has recommended a move towards high availability architecture to address this. What is the PRIMARY concern when implementing high availability?

- (A) Ensuring that there are no single points of failure
- (B) Ensuring that the system is patched regularly
- (C) Implementing multi-factor authentication
- (D) Storing backups in multiple geographical locations

Question 40. In a cloud environment, which of the following matrices defines the shared responsibilities between the cloud provider and the customer for specific cloud service models?

- (A) Shared Accountability Matrix
- (B) Cloud Resource Allocation Table
- (C) Cloud Security Posture Matrix
- (D) Cloud Responsibility Matrix

Question 41. A multinational company is planning to issue company-owned mobile devices to its executives. Given the

sensitivity of the data the executives handle, what hardening measure would be MOST effective to ensure the security of these mobile devices?

- (A) Regularly updating the company's social media profiles to mention the security measures taken
- (B) Implementing biometric authentication in addition to strong passcodes
- (C) Turning off Bluetooth and Wi-Fi when not in use
- (D) Setting the devices to display brighter screen colors

Question 42. A multinational company is deploying a new set of servers in its data centers across various countries. Which of the following steps should be taken FIRST to ensure the servers are secured against potential threats?

- (A) Set up a monitoring system to alert the IT team of any irregular activities
- (B) Deploy all the software applications the company might need in the future
- (C) Use the server's default configuration to ensure manufacturer's best practices are maintained
- (D) Disable any unused services and ports on the server

Question 43. During an incident response, the IT team discovers malware that collects information about military projects. The malware sends the data to a server located in a foreign country. Which type of threat actor would MOST likely be involved in this type of cyber espionage?

- (A) Disgruntled employee
- (B) Nation-state
- (C) Phishing scam artist
- (D) Hacktivist

Question 44. A large e-commerce platform is facing challenges during peak sale periods, where the influx of users causes slowdowns and occasional outages. Which of the following solutions would BEST improve scalability during these high-demand times?

- (A) Implement a centralized logging system
- (B) Employ auto-scaling cloud solutions
- (C) Increase the frequency of data backups
- (D) Mandate regular security training for employees

Question 45. A large enterprise is considering a transition to a more flexible and programmable network architecture. They want to centralize the control plane, allowing for automated, programmable network configurations and rapid provisioning. Which network architecture model should they consider?

- (A) VLAN (Virtual Local Area Network)
- (B) MPLS (Multiprotocol Label Switching)
- (C) VPN (Virtual Private Network)
- (D) SDN (Software-Defined Networking)

Question 46. An audit report indicates that several network switches in a data center lack security configurations, making them potential targets for attackers. Which of the following hardening techniques would BEST reduce the risk associated with these switches?

- (A) Configuring port mirroring to monitor network traffic
- (B) Disabling unused switch ports
- (C) Implementing load balancing across the switches
- (D) Increasing the MAC address table size for performance

Question 47. An e-commerce platform reported a series of breaches over the past month. With each breach, financial and personal data of thousands of users were exfiltrated. The perpetrators subsequently sold the data on the dark web. Which type of threat actor is MOST likely behind these breaches?

- (A) Insider threat
- (B) Hacktivist
- (C) Organized crime syndicate
- (D) Nation-state

Question 48. A company's primary security control for accessing secure server rooms is a biometric fingerprint scanner. However, the scanner occasionally malfunctions in high humidity. The security team is considering an alternative solution to grant access when the primary method fails. Which of the following would be the MOST appropriate compensating control?

- (A) Implementing a security token-based authentication system
- (B) Employing security guards at the main entrance
- (C) Installing security cameras inside the server room
- (D) Conducting regular server room audits

Question 49. A medium-sized financial firm has noticed a series of unauthorized transactions moving funds from legitimate accounts to overseas locations. After investigating, it was found that a group was responsible for exploiting vulnerabilities in the firm's transaction system. Which of the following motivations is most likely driving this group's actions?

- (A) Seeking notoriety within the hacker community

- (B) Financial gain from unauthorized transactions
- (C) Demonstrating political beliefs against financial institutions
- (D) Espionage to uncover the firm's investment strategies

Question 50. TechGuard Corp. conducts a risk assessment every six months to identify new vulnerabilities and ensure that previous risk-mitigation strategies remain effective. This type of risk assessment is best described as:

- (A) Periodic
- (B) Ad hoc
- (C) Continuous
- (D) Recurring

Question 51. An e-commerce company recently faced a DDoS attack that rendered its website unavailable for several hours. While reflecting on the incident, the CISO emphasized the importance of having a detailed plan that includes identification, containment, eradication, recovery, and lessons learned. Which policy primarily encompasses these stages for handling security incidents?

- (A) Change Management Policy
- (B) Incident Response Policy
- (C) Disaster Recovery Policy
- (D) Remote Access Policy

Question 52. MatrixCorp recently adopted a mobile strategy where employees are provided with company-owned devices. These devices are also allowed for personal use, but the organization retains the ability to manage and monitor them. Which deployment model is MatrixCorp using?

- (A) Bring Your Own Device (BYOD)
- (B) Choose Your Own Device (CYOD)
- (C) Corporate-owned, Personally Enabled (COPE)
- (D) Public Device Deployment (PDD)

Question 53. The network administrator of a rapidly growing tech firm is concerned about the potential vulnerabilities of the company's switches. Which of the following measures is MOST effective in hardening these network switches against possible attacks?

- (A) Assigning static IP addresses to all connected devices
- (B) Implementing strong password policies for switch access
- (C) Upgrading the switches to support 10Gbps for future expansion
- (D) Customizing the switch LED colors for easy identification

Question 54. A developer at your company is excited about the scalability benefits of serverless architecture and has deployed a new service using it. However, you notice an increased bill due to the service even when it's not in use. Which of the following could be a contributing factor?

- (A) The serverless functions are continuously triggered by unintended events
- (B) The server hardware is outdated
- (C) The load balancer is misconfigured
- (D) The organization lacks a Content Delivery Network (CDN)

Question 55. AlphaTech wants to ensure that its remote employees follow best security practices when working from home. The security team has been tasked with drafting a set of guidelines for remote work. What should be the primary focus of these guidelines?

- (A) Outlining punitive measures for non-compliance
- (B) Stating the company's legal position on remote work
- (C) Recommending security measures for home networks and devices
- (D) Dictating the exact software and hardware specifications for remote workers

Question 56. Lisa, a security manager, is reviewing the company's existing policies and realizes that there isn't a comprehensive document detailing the organization's stance, expectations, and commitment to protecting its information assets. Which of the following should Lisa prioritize creating to address this gap?

- (A) Incident Response Plan
- (B) Information Security Policy
- (C) Acceptable Use Policy
- (D) Data Backup Strategy

Question 57. GlobalFin, a fintech company, has developed a new mobile banking application. To avoid any legal complications, which of the following legal external considerations should GlobalFin pay the most attention to before launching the application worldwide?

- (A) Ensuring the app meets global data privacy laws
- (B) Confirming the color scheme aligns with branding regulations in all countries

- (C) Securing copyrights for all images used in the app
- (D) Making sure the app's name isn't offensive in any language

Question 58. In a microservices architecture, each service should be designed with a specific principle to ensure it performs a specific task and interacts with other services through well-defined interfaces. What principle is this referring to?

- (A) Principle of Least Privilege
- (B) Single Responsibility Principle
- (C) Open-Closed Principle
- (D) Zero Trust Model

Question 59. XYZ Corp is in the process of defining clear roles and responsibilities for their IT assets. During a meeting, the team discussed the primary individual who will have the responsibility for the data within a specific IT system and also be the main point of contact for any decisions related to it. Which of the following roles best describes this individual?

- (A) System administrator
- (B) Data custodian
- (C) System owner
- (D) End-user

Question 60. An organization with a single physical network infrastructure wants to separate the traffic of its finance department from that of the HR department. They do not want to set up entirely new physical networks but want to ensure that data packets from one department do not mix with the other's. What should the organization implement?

- (A) Air-gapped network
- (B) DMZ (Demilitarized Zone)
- (C) VLAN (Virtual Local Area Network)
- (D) VPN (Virtual Private Network)

Question 61. A medium-sized company suffered a data breach. Investigations revealed that an attacker from a rival firm had exploited a misconfigured firewall to gain unauthorized access to the company's database. Based on the attributes of the actor, how would this threat actor be best described?

- (A) Internal actor leveraging physical access
- (B) Internal actor abusing privileges
- (C) External actor using social engineering
- (D) External actor exploiting technical vulnerabilities

Question 62. A global corporation has undergone several IT incidents in the past year, including outages due to natural disasters and cyber attacks. The CEO wants to ensure the organization's IT infrastructure can withstand or rapidly recover from disruptive events. Which of the following best encapsulates this requirement?

- (A) Adopting a Zero Trust Architecture
- (B) Implementing a strict password policy
- (C) Establishing a Business Continuity Plan (BCP) with emphasis on resilience
- (D) Regularly updating firewall rules

Question 63. A company has faced multiple instances of unauthorized individuals gaining access to their office premises. Which of the following preventive security controls would be MOST effective in preventing unauthorized physical access?

- (A) Implementing a log monitoring solution for network traffic
- (B) Installing video surveillance cameras at all entry and exit points
- (C) Conducting regular security awareness training for employees
- (D) Implementing a multi-factor authentication system for network access.

Question 64. After detecting an unauthorized intrusion into their network, a financial institution wants to implement a control that will restore compromised systems to a known good state. Which of the following would be the MOST appropriate corrective control?

- (A) Implementing Intrusion Detection Systems (IDS) across the network
- (B) Frequently updating firewall rules
- (C) Restoring systems from verified backups
- (D) Enabling multi-factor authentication for users

Question 65. An organization that processes classified information is implementing a network infrastructure to ensure the highest level of data security. The CISO recommends using a network configuration that ensures the system remains completely disconnected from unsecured networks and any external connections. Which of the following describes this type of configuration?

- (A) DMZ (Demilitarized Zone)
- (B) VPN (Virtual Private Network)
- (C) VLAN (Virtual Local Area Network)
- (D) Air-gapped network

Question 66. A small business detected unauthorized access to its website. The attacker used default login credentials to gain access. What level of sophistication and capability does this attack suggest about the threat actor?

- (A) Script kiddie with basic skills
- (B) Expert attacker leveraging advanced techniques
- (C) Nation-state actor with strategic objectives
- (D) Organized crime syndicate targeting high-value assets

Question 67. To discourage potential cybercriminals from targeting their online storefront, an e-commerce company is considering various security measures. Which of the following would act MOST effectively as a deterrent control?

- (A) Displaying a seal for third-party security certifications on the website
- (B) Using a Web Application Firewall (WAF)
- (C) Conducting monthly vulnerability assessments
- (D) Storing customer data in encrypted databases

Question 68. A system administrator is setting up an authentication system for a new web application. Which of the following security controls falls under the technical category and ensures that users prove their identity before gaining access?

- (A) Implementing a security awareness training program
- (B) Conducting a background check for new employees
- (C) Using multi-factor authentication
- (D) Establishing a clean desk policy

Question 69. CyberFirm, a leading software development company, recently updated their server OS due to new features

and patches. Given that they have already established and deployed a secure baseline in the past, what should CyberFirm do NEXT to ensure continued security?

- (A) Conduct a complete system reboot for all servers
- (B) Re-deploy the same baseline without any modifications
- (C) Update the secure baseline to include new configurations and then deploy it
- (D) Implement a new firewall rule for the servers

Question 70. A cybersecurity analyst has noticed a series of sophisticated attacks against critical infrastructure systems in their country. The attacks are highly coordinated, well-funded, and appear to have specific geopolitical objectives. Which type of threat actor is MOST likely responsible for these attacks?

- (A) Organized crime syndicates
- (B) Script kiddies
- (C) Insider threat
- (D) Nation-state

Question 71. An e-commerce company is preparing for an upcoming Black Friday sale, expecting a surge in web traffic. To ensure their systems remain responsive during the sale, which of the following would be the MOST effective strategy to implement?

- (A) Increasing password complexity for all users
- (B) Limiting the number of products on sale
- (C) Implementing a content delivery network (CDN)
- (D) Conducting a yearly security audit

Question 72. Alice wants to access a restricted online portal. The portal asks her to enter a unique username and a secret passphrase only she should know. This process helps the system ensure that Alice is who she claims to be. What security concept is the portal employing?

- (A) Authorization
- (B) Accounting
- (C) Multifactor authentication
- (D) Authentication

Question 73. During a routine check, the IT department discovered that several employees had left their computers on and unattended during lunch break. Which operational security control can help mitigate the risk associated with this behavior?

- (A) Implementing biometric authentication
- (B) Enforcing a strict password policy
- (C) Deploying an automatic screen lock after inactivity
- (D) Implementing a secure coding practice

Question 74. A retail company recently suffered a breach where attackers encrypted all point-of-sale systems, rendering them unusable. A ransom note was then received, demanding payment in cryptocurrency to decrypt the systems. What motivation is most evident behind this attack?

- (A) Protesting against the company's environmental policies
- (B) Financial gain through ransom
- (C) Espionage to understand the company's supply chain
- (D) Seeking a reputation boost by showing off technical skills

Question 75. In an effort to minimize data breaches from malware, a company is deciding on a control to prevent malicious software from being executed on company devices. Which of the following would be the BEST preventive control?

- (A) Deploying a Network Intrusion Detection System (NIDS)
- (B) Regularly backing up critical data
- (C) Installing an antivirus software with real-time scanning
- (D) Performing a forensic analysis after a security incident

Question 76. After a recent service outage, a hospital's IT team is reviewing the availability of its patient record system. They want to ensure the system remains operational, even in the event of hardware failures. Which of the following considerations is MOST relevant to this requirement?

- (A) Implementing database mirroring
- (B) Regularly updating the system's antivirus definitions
- (C) Using strong encryption for data at rest
- (D) Conducting penetration testing on the system

Question 77. An environmental NGO's website was hacked and replaced with a message decrying their recent campaign against deforestation, claiming they are spreading misinformation. The website was left with a manifesto promoting responsible forestry and sustainable logging practices. Which type of threat actor is MOST likely behind this incident?

- (A) Ransomware gang
- (B) Organized crime syndicate

- (C) Hacktivist
- (D) Advanced Persistent Threat (APT)

Question 78. A government agency experienced a cyber incident where its communication platforms were breached. The intruders were not interested in extracting sensitive data or causing disruptions but were observed to be silently monitoring diplomatic communications for an extended period. What was the likely motivation of the attackers?

- (A) To gain financial benefits from insider trading
- (B) Espionage to understand and anticipate diplomatic moves
- (C) Disgruntlement of an internal employee
- (D) An attempt to expand their cybercriminal network

Question 79. During a company's onboarding process, new employees are required to read and acknowledge understanding of various company policies. The HR department wants to ensure that employees are aware of their responsibilities when it comes to the use of company devices and internet resources. Which policy should be included in the onboarding packet to address this?

- (A) Password Complexity Policy
- (B) Data Classification Policy
- (C) Acceptable Use Policy (AUP)
- (D) Vendor Management Policy

Question 80. WhiteCape Healthcare, an international healthcare provider, has a large patient database that includes many EU citizens. They're about to implement a new system to improve data access for physicians. Which of the following regulatory

requirements should they pay particular attention to when granting physicians access to EU patient data?

- (A) Ensure data is only accessed for tax reporting purposes
- (B) Acquire explicit consent from patients before sharing data
- (C) Encrypt all data using a proprietary algorithm
- (D) Store data in a physical server located within the EU

Question 81. An enterprise is deploying IoT-based security cameras across multiple office locations. As the lead security professional, what recommendation would you prioritize to establish a secure baseline for these devices?

- (A) Setting the devices to public mode so all employees can access the feed for transparency
- (B) Regularly updating the device firmware to patch known vulnerabilities
- (C) Enabling Universal Plug and Play (UPnP) to ensure easy connectivity for all devices on the network
- (D) Using the same password for all cameras for ease of management

Question 82. A robotics company is developing an autonomous vehicle that relies on a Real-Time Operating System (RTOS) to manage its operations. The development team wants to ensure that the vehicle's RTOS has a solid security posture. What should the team prioritize when establishing a secure baseline for this RTOS?

- (A) Installing a robust antivirus software
- (B) Enabling all features for maximum functionality
- (C) Regularly backing up the RTOS data to the cloud
- (D) Minimizing the number of services and open ports

Question 83. After a recent incident of vandalism, a corporate building is considering implementing security controls that would dissuade potential perpetrators. Which of the following would serve BEST as a deterrent control?

- (A) Encrypting all stored data
- (B) Installing biometric access controls on all entrances
- (C) Implementing regular data backups
- (D) Placing visible security signage indicating 24/7 surveillance

Question 84. The finance department of a global corporation found a series of unauthorized transactions originating from an employee's workstation. Investigations revealed that the employee had been bypassing company policies to make unauthorized investments using company funds. Based on the attributes of the actor, how can this threat actor be best categorized?

- (A) External actor leveraging malware
- (B) External actor exploiting vulnerabilities
- (C) Internal actor with direct access
- (D) Internal actor with indirect access

Question 85. After a series of cyberattacks, BetaTech, a financial institution, decided to standardize the configurations across its entire server fleet. They've established a secure baseline configuration for their servers. What should be the NEXT step in ensuring the servers conform to this new baseline?

- (A) Frequently conduct vulnerability scanning on all servers
- (B) Introduce biometric authentication for server access

- (C) Deploy the secure baseline across all servers
- (D) Monitor network traffic to detect anomalies

Question 86. ClearView Industries wants to give their employees the flexibility to choose their own devices for work while retaining control over the device configurations and applications. Which deployment model would be the MOST appropriate for ClearView's objectives?

- (A) Bring Your Own Device (BYOD)
- (B) Choose Your Own Device (CYOD)
- (C) Corporate-owned, Personally Enabled (COPE)
- (D) Fixed Device Deployment (FDD)

Question 87. XYZ Company uses MDM to manage company-owned and employee-owned mobile devices. An employee reported losing their personal phone over the weekend. What MDM feature should the IT department use to ensure that sensitive company data on the lost phone isn't accessed?

- (A) Monitor the device's location
- (B) Force update the device's apps
- (C) Remote wipe the device
- (D) Change the user's email password

Question 88. During a major sports event, a broadcasting company's streaming services were taken offline by a sudden surge in traffic. The attack continued for the duration of the event and then subsided. What was the most probable motivation behind this attack?

- (A) Espionage to intercept sensitive communications
- (B) To cause a service disruption during the sports event

- (C) Data exfiltration for future ransom demands
- (D) To gain unauthorized access and implant malware

Question 89. A software development company has decided to host their applications in a multi-cloud environment. Before deploying, they are looking to enhance the security of their cloud-based resources. Which of the following is the BEST practice for hardening their cloud infrastructure?

- (A) Ensure that all cloud storage buckets or containers are publicly accessible for easier data sharing
- (B) Apply consistent security configurations and policies across all cloud providers
- (C) Use the same SSH key pairs across all cloud instances for uniformity
- (D) Limit the use of Identity and Access Management (IAM) roles to senior staff only

Question 90. RedFlare Solutions, a financial firm, is storing sensitive client data in a database. The Chief Information Security Officer (CISO) insists that the data should be unreadable even if it's intercepted during transmission or if the storage is compromised. Which encryption standard would best serve this requirement?

- (A) Symmetric encryption using a shared key
- (B) Hashing the data with a one-way function
- (C) Encrypting the entire database using transparent data encryption
- (D) Storing the data in a proprietary format

Question 91. XYZ Corporation is planning to deploy a new wireless infrastructure in their newly acquired office building.

The IT manager wants to ensure optimal wireless coverage throughout the premises. Which of the following should the IT team prioritize before installing the wireless access points?

- (A) Purchase the most expensive wireless access points to ensure maximum range
- (B) Conduct a site survey to determine the best locations for access points
- (C) Deploy all access points near windows to enhance signal strength
- (D) Ensure all users have 5GHz capable devices

Question 92. A client disputes having signed a digital contract. The service provider needs to prove that the signature was indeed from the client and hasn't been tampered with. Which of the following security concepts is the service provider relying on?

- (A) Authentication
- (B) Confidentiality
- (C) Non-repudiation
- (D) Access Control

Question 93. A software company recently discovered a vulnerability in its popular application, which allowed unauthorized access to users' data. Before the company could release a patch, a group of hackers exploited the vulnerability but only to notify the users about it. They did not misuse any data. What is the most probable motivation behind this group's action?

- (A) Financial gain by selling the data
- (B) Political beliefs against the software company's operations

- (C) Ethical concerns about user privacy and security
- (D) Desire to disrupt the software company's services

Question 94. A healthcare institution suffered a breach where medical records of high-profile patients were extracted. The data was not sold or publicly disclosed. Instead, certain individuals were approached with their personal health information and were extorted for money. What is the primary motivation behind this cyber attack?

- (A) Political activism to expose vulnerabilities in healthcare
- (B) Personal animosity targeting the healthcare institution
- (C) Financial gain through targeted extortion
- (D) Spreading malware and expanding the botnet

Question 95. A company wants to ensure that security incidents are detected and addressed as quickly as possible by on-duty personnel. Which of the following operational security controls would be BEST to implement for this purpose?

- (A) Deploying a Network Intrusion Prevention System (NIPS)
- (B) Establishing a 24/7 Security Operations Center (SOC)
- (C) Creating a company-wide security policy
- (D) Implementing end-to-end data encryption

Question 96. As part of improving their security posture, TechHive Inc. decided to review their existing password policies. The current policy requires employees to use at least one uppercase letter, one number, and one special character. However, they found that users mostly only make minimal changes to their passwords during resets. Which standard should be integrated into their policy to ensure passwords are

more complex and unique over time?

- (A) Password history retention
- (B) Password expiration period
- (C) Account lockout duration
- (D) Maximum password age

Question 97. A medium-sized enterprise is concerned about the security of its office workstations after a series of malware infections. As a security analyst, which of the following recommendations would BEST improve the security baseline of the workstations?

- (A) Install multiple antivirus solutions to ensure maximum detection
- (B) Set up screensavers with cyber hygiene tips to educate users
- (C) Disable unnecessary services and ports on the workstations
- (D) Frequently change the desktop wallpaper to prevent monotony

Question 98. After a significant merger between two large corporations, a comprehensive risk assessment was conducted to identify potential security gaps within the combined infrastructure. This assessment was exclusive to the merger and was not planned to be repeated in the future. What type of risk assessment was this?

- (A) Recurring
- (B) Continuous
- (C) One-time
- (D) Dynamic

Question 99. XYZ Corporation recently faced a major power outage that affected their primary data center. During the incident, it was found that there was no clear guidance on the steps to maintain or quickly restore business operations. To address this, which of the following policies should XYZ Corporation prioritize implementing?

- (A) Data Classification Policy
- (B) Business Continuity Policy
- (C) Acceptable Use Policy
- (D) Network Segmentation Strategy

Question 100. CyberFleet Inc., a software development company, has just heard of a newly discovered vulnerability in a third-party library they heavily rely upon. The security team quickly gathers to understand and analyze the potential risks associated with this vulnerability. This spontaneous assessment is best described as:

- (A) Routine
- (B) Ad hoc
- (C) Scheduled
- (D) Benchmark

Answers 1-100

Question 1. A smart city project is deploying various IoT sensors across the city to gather data on traffic patterns, weather, pollution levels, and more. Which of the following is the MOST critical security consideration when deploying these sensors?

- (A) Ensuring high data transfer speeds to cater to the volume of data from the IoT sensors
- (B) Limiting the IoT devices to communicate only with specific, pre-defined servers**
- (C) Installing physical locks on IoT devices to prevent theft
- (D) Allowing IoT devices to connect to any available network for data redundancy

Explanation 1. Correct Answer: B. Limiting the IoT devices to communicate only with specific, pre-defined servers. By restricting IoT devices to communicate only with specific, trusted servers, unauthorized access and data tampering risks can be minimized. This measure ensures that data is only sent to and received from legitimate sources.

Option A is incorrect. While data transfer speeds are important for performance and real-time analytics, from a security standpoint, the integrity and confidentiality of the data is more crucial.

Option C is incorrect. While physical security is an essential aspect, especially in a public setting, the most significant risks with IoT often pertain to data security and unauthorized access.

Option D is incorrect. Allowing IoT devices to connect to any available network can introduce significant security

vulnerabilities, such as man-in-the-middle attacks, eavesdropping, or unauthorized data tampering.

Question 2. TechFirm Inc. has decided to engage in a new business venture. Before they move forward, the security team conducts several brainstorming sessions, interviews, and reviews historical data to generate a list of potential security threats that the new venture could face. This activity is a primary component of which step in the risk management process?

- (A) Risk assessment
- (B) Risk response
- (C) Risk monitoring
- (D) **Risk identification**

Explanation 2. Correct Answer: D. Risk identification. Risk identification is the initial process of detecting and describing risks that could potentially affect the achievement of objectives.

Option A is incorrect. Risk assessment encompasses the overall process of identifying, analyzing, and evaluating risks, but the specific activity mentioned is related to risk identification.

Option B is incorrect. Risk response involves deciding on the most suitable approach to address identified risks, whether it's accepting, avoiding, transferring, or mitigating them.

Option C is incorrect. Risk monitoring is about tracking identified risks, monitoring residual risks, and identifying new

risks. The specific activity of brainstorming and gathering data about risks falls under risk identification.

Question 3. A large financial organization wants to ensure that all employees understand the importance of cybersecurity and the role they play in safeguarding company assets. Which of the following managerial security controls will be MOST effective in achieving this?

- (A) Installing a firewall at the network perimeter
- (B) **Regular security awareness training for employees**
- (C) Deploying an Intrusion Detection System (IDS)
- (D) Encrypting all company data

Explanation 3. Correct Answer: B. Regular security awareness training for employees. Security awareness training is a managerial control aiming to educate employees about security risks and the necessary precautions they need to take. By regularly training employees, the organization ensures that all staff are aware of potential threats and their roles in cybersecurity.

Option A is incorrect. Installing a firewall is a technical control focused on preventing unauthorized access to or from a private network. While it protects the network, it doesn't directly educate employees about their roles in cybersecurity.

Option C is incorrect. Deploying an Intrusion Detection System (IDS) is a technical control. It monitors network traffic for suspicious activities but does not directly focus on educating employees.

Option D is incorrect. Encrypting company data is a technical control. While it ensures the confidentiality of data, it doesn't address the employees' knowledge or awareness regarding cybersecurity.

Question 4. A major pharmaceutical company recently announced an increase in drug prices. Following the announcement, their website was taken offline by a DDoS attack, with a message posted online by a group claiming responsibility and demanding affordable healthcare for all. Which type of threat actor is MOST likely behind this attack?

- (A) Unskilled attacker
- (B) Insider threat
- (C) **Hactivist**
- (D) Nation-state

Explanation 4. Correct Answer: C. Hactivist. Hacktivists are typically driven by political, social, or ideological motives. They use cyber attacks as a means to promote or protest certain issues. In this scenario, the attack on the pharmaceutical company is a form of protest against their pricing policies, making it characteristic of hacktivist behavior.

Option A is incorrect. Unskilled attackers generally conduct attacks for personal bragging rights or mischief. They are not usually driven by ideological motives like demanding affordable healthcare.

Option B is incorrect. Insider threats stem from individuals within the organization, often driven by personal grievances or

financial gain. The described scenario shows a motive tied to a broader social issue, not a personal or internal motive.

Option D is incorrect. Nation-states conduct cyber operations for political, espionage, or military reasons. Protesting drug prices is not in line with their typical objectives.

Question 5. After deploying wireless access points in a large manufacturing facility, employees report inconsistent wireless connectivity in some areas. What tool would be most effective for the IT team to use to visualize areas of weak wireless signal strength?

- (A) Network bandwidth monitor
- (B) Protocol analyzer
- (C) **Heat map software**
- (D) Intrusion detection system

Explanation 5. Correct Answer: C. Heat map software. Heat map software allows IT professionals to visually see areas of strong and weak wireless signal strength, making it easier to adjust placements or add additional access points as needed.

Option A is incorrect. A network bandwidth monitor is used to measure the amount of data being sent over a network, not to visualize wireless signal strength.

Option B is incorrect. A protocol analyzer is used to capture and analyze network traffic, not to visually display wireless coverage.

Option D is incorrect. An intrusion detection system (IDS) is designed to detect unauthorized access or malicious activities on a network. It does not show areas of weak wireless signal strength.

Question 6. In an IaaS (Infrastructure as a Service) model, which of the following tasks is typically the responsibility of the cloud customer in a standard Cloud Responsibility Matrix?

- (A) Physical security of data centers
- (B) Patching of host operating systems
- (C) Network infrastructure maintenance
- (D) **Patching of guest operating systems**

Explanation 6. Correct Answer: D. Patching of guest operating systems. In an IaaS model, the customer is typically responsible for managing their own virtual machines, which includes patching the guest operating systems. The cloud provider is generally responsible for the physical infrastructure, network, and the host operating system.

Option A is incorrect. Physical security of data centers is the responsibility of the cloud provider. The customer does not have control over the physical infrastructure in a cloud environment.

Option B is incorrect. Patching of host operating systems is the cloud provider's responsibility. They manage the underlying infrastructure, including the host systems.

Option C is incorrect. Maintenance of network infrastructure is typically handled by the cloud provider, ensuring connectivity and uptime for the resources they offer.

Question 7. A company's website was temporarily defaced with a humorous meme, but no sensitive data was stolen or any significant damage done. The attacker left a message bragging about their first successful hack. Which type of threat actor is MOST likely responsible for this attack?

- (A) Insider threat
- (B) Advanced Persistent Threat (APT)
- (C) **Unskilled attacker**
- (D) Nation-state

Explanation 7. Correct Answer: C. Unskilled attacker.

Unskilled attackers, often referred to as “script kiddies”, typically utilize pre-made tools or scripts to carry out basic attacks. Their motivations are often more about bragging rights or minor mischief, such as defacing a website for fun or to prove they can, rather than executing a sophisticated or damaging attack.

Option A is incorrect. Insider threats are individuals within an organization that may have specific motives related to personal grievances or financial gain. Their attacks would typically be more targeted and potentially more harmful than just defacing a website.

Option B is incorrect. Advanced Persistent Threats (APTs) are highly skilled and typically represent organized groups with specific, long-term objectives. Their attacks are sophisticated and stealthy, aiming for data theft or system compromise over an extended period.

Option D is incorrect. Nation-states are motivated by political, military, or espionage objectives. A simple website defacement, especially one with a humorous meme, does not align with their typical motivations or methods.

Question 8. A financial institution recently discovered that a large number of confidential customer records were being accessed and copied during off-business hours. Upon investigation, it was found that the access came from an authenticated user within the company, who had recently been passed over for a promotion. Which type of threat actor is MOST likely responsible for this security incident?

- (A) Hacktivist
- (B) **Insider threat**
- (C) Nation-state
- (D) Organized crime syndicate

Explanation 8. Correct Answer: B. Insider threat. The evidence suggests the activities were conducted by an authenticated user within the organization, who might have a motive (having been passed over for a promotion). Insider threats are risks from individuals within the organization such as employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems.

Option A is incorrect. Hacktivists are typically motivated by political or social causes and will target organizations to promote or protest a specific issue. They are not usually motivated by personal grievances like being passed over for promotions.

Option C is incorrect. Nation-states are driven by political, espionage, or military objectives. Accessing customer records of a financial institution for personal reasons doesn't align with their typical motivations.

Option D is incorrect. While organized crime syndicates might have an interest in customer records for financial gains, the inside access and the motive related to a missed promotion strongly suggest an insider threat.

Question 9. A company is evaluating its data storage options. They need a solution that provides them with the highest level of control over their hardware, software, and network configurations, allowing for customized security controls and measures. Which deployment model would best suit their needs?

- (A) Cloud-based Infrastructure
- (B) Hybrid Infrastructure
- (C) **On-premises Infrastructure**
- (D) Community Cloud

Explanation 9. Correct Answer: C. On-premises Infrastructure. On-premises infrastructure allows organizations to have complete control over their hardware, software, and network configurations. This gives them the freedom to customize security controls and measures tailored to their specific needs.

Option A is incorrect. Cloud-based infrastructures are hosted by third-party providers, which means organizations might not

have the same level of control or customization over their resources.

Option B is incorrect. Hybrid infrastructure combines on-premises and cloud resources. While it offers more control than purely cloud-based solutions, it still doesn't provide the total control that on-premises infrastructure does.

Option D is incorrect. A community cloud is shared by several organizations with similar requirements. While it offers some level of control, it doesn't provide the complete customization and control that an on-premises infrastructure does.

Question 10. A new technology firm recently launched a device that uses facial recognition for authentication. A cybersecurity researcher, without any malicious intent, demonstrated a method to bypass the facial recognition using a photograph. The researcher then approached the firm with the findings without publicizing it. What is the primary motivation behind the researcher's action?

- (A) Philosophical beliefs opposing facial recognition
- (B) Financial gain by blackmailing the firm
- (C) **Ethical considerations for consumer security**
- (D) Aiming to damage the firm's market reputation

Explanation 10. Correct Answer: C. Ethical considerations for consumer security. By responsibly disclosing the vulnerability to the firm without any malicious intent or publicizing it, the researcher showcased ethical motivations, aiming to improve consumer security.

Option A is incorrect. The researcher did not express opposition to facial recognition technology but only highlighted a potential vulnerability.

Option B is incorrect. There is no evidence that the researcher tried to blackmail the firm. Instead, they responsibly disclosed the vulnerability.

Option D is incorrect. The researcher chose not to publicize the vulnerability, indicating they were not aiming to damage the firm's reputation but to assist in improving security.

Question 11. ABC Corp recently adopted a Bring Your Own Device (BYOD) policy. The IT department is concerned about the potential risks associated with personal devices accessing the corporate network. Which of the following solutions would be MOST effective for enforcing security policies on these personal mobile devices?

- (A) Installing antivirus software on each device
- (B) Establishing a separate guest Wi-Fi network for mobile devices
- (C) **Using Mobile Device Management (MDM) to enforce security policies**
- (D) Mandating that employees use strong passwords on their personal devices

Explanation 11. Correct Answer: C. Using Mobile Device Management (MDM) to enforce security policies. MDM solutions provide centralized control to enforce security policies, manage device features, and ensure that personal

devices meet the organization's security standards before accessing corporate resources.

Option A is incorrect. While installing antivirus software is a good security measure, it doesn't provide the comprehensive policy enforcement capabilities that MDM does.

Option B is incorrect. A separate guest Wi-Fi may restrict access to the internal network, but it doesn't manage or enforce security policies on the devices themselves.

Option D is incorrect. While using strong passwords is essential, it's just one aspect of device security. MDM offers broader policy enforcement capabilities.

Question 12. AcmeTech, a software development firm, recently experienced a major data breach that was traced back to a vulnerability in their custom-built application. Post-incident analysis revealed that the vulnerability had been introduced during the coding phase and was never detected during testing. To avoid such vulnerabilities in the future, which policy should AcmeTech emphasize to ensure secure practices are maintained throughout the development process?

- (A) Incident Response Policy
- (B) Change Management Policy
- (C) Business Continuity Policy
- (D) **Software Development Lifecycle (SDLC) Policy**

Explanation 12. Correct Answer: D. Software Development Lifecycle (SDLC) Policy. The Software Development Lifecycle (SDLC) Policy provides guidelines and standards for each

phase of the software development process, ensuring that security is integrated at every step, from requirement gathering to deployment and maintenance.

Option A is incorrect. While an Incident Response Policy provides a structured approach to manage and respond to security incidents, it does not focus on the software development process.

Option B is incorrect. The Change Management Policy deals with procedures for implementing changes in the IT environment but doesn't specifically cater to the development of software applications.

Option C is incorrect. A Business Continuity Policy focuses on maintaining business operations during and after a disruption and doesn't address the specifics of software development.

Question 13. A high-profile executive received an email containing personal photos and a message threatening to release the images to the public unless a significant sum of money was transferred to a specific cryptocurrency address. What motivation is most evident behind this threat?

- (A) Espionage to gather competitive intelligence
- (B) Service disruption to harm the reputation of the executive's company
- (C) **Blackmail to extract money by leveraging sensitive information**
- (D) Data exfiltration for selling on the dark web

Explanation 13. Correct Answer: C. Blackmail to extract money by leveraging sensitive information. The direct threat of releasing personal photos in exchange for money is a classic indication of blackmail. The attacker is leveraging sensitive information (personal photos) to extort money.

Option A is incorrect. There's no mention of seeking company secrets or competitive intelligence. The focus of the attacker is on personal images of the executive.

Option B is incorrect. While releasing the images might harm the executive's reputation, there's no direct intent shown to disrupt the company's services or harm its operational standing.

Option D is incorrect. The attacker is directly demanding money in exchange for not releasing the photos. This differs from data exfiltration where data might be sold or leveraged in other ways.

Question 14. A software development team in a large corporation decided to use an unauthorized cloud-based tool to host and manage their source code. The team believed it would increase their productivity, even though it was not approved by the IT department. A few weeks later, unauthorized access to their project data was detected. Which threat actor concept BEST describes the situation?

- (A) Insider threat
- (B) Hacktivist
- (C) **Shadow IT**
- (D) Organized crime syndicate

Explanation 14. Correct Answer: C. Shadow IT. Shadow IT refers to any IT systems or solutions used within an organization without organizational approval or oversight. This can introduce vulnerabilities, as the unauthorized systems might not meet the security standards set by the organization's IT department. In this scenario, the software development team's unauthorized use of a cloud tool exemplifies Shadow IT.

Option A is incorrect. While the software development team acted without approval, their intention was to increase productivity, not to harm the organization. Therefore, this situation does not fit the typical definition of an "insider threat," which usually has malicious intent.

Option B is incorrect. Hacktivists are motivated by political or social causes. There's no evidence in the scenario to suggest that political or social motivations were behind the team's decision.

Option D is incorrect. While the data was accessed without authorization, there's no evidence to suggest that this was the work of an organized crime syndicate. The main issue at hand is the unauthorized use of IT resources, which is a hallmark of Shadow IT.

Question 15. A financial institution has experienced an uptick in unauthorized transactions. They want to implement a control that will allow them to identify suspicious transactions in real-time. Which of the following would be the BEST detective control for this scenario?

(A) Implementing a multi-factor authentication system for

all users

- (B) Establishing a Security Operations Center (SOC) to monitor network traffic
- (C) **Installing an Intrusion Detection System (IDS) on their network**
- (D) Restricting transaction capabilities to only a few trusted IP addresses.

Explanation 15. Correct Answer: C. Installing an Intrusion Detection System (IDS) on their network. An Intrusion Detection System (IDS) serves as a detective control by monitoring network traffic for suspicious activities and potential threats. In this context, it can be configured to detect patterns related to unauthorized transactions, thereby allowing timely intervention.

Option A is incorrect. Implementing a multi-factor authentication system is a preventive control that provides an additional layer of security by requiring two or more verification methods. While it reduces the risk of unauthorized access, it does not detect suspicious transactions.

Option B is incorrect. Establishing a Security Operations Center (SOC) is a broad approach to handle security events, and while it can include detective controls, merely setting up a SOC does not provide specific real-time detection of unauthorized transactions.

Option D is incorrect. Restricting transaction capabilities to only a few trusted IP addresses is a preventive control that limits the sources of potential transactions. While it can reduce

the number of unauthorized transactions, it does not detect them.

Question 16. MegaTech Inc. is in the process of outlining a strategy to ensure that after any disaster, critical applications can be restored to a working state within 4 hours. The organization also wants to make sure that the data loss does not exceed 1 hour. Which of the following policies is most relevant to achieving this objective?

- (A) Data Retention Policy
- (B) Incident Response Policy
- (C) **Disaster Recovery Policy**
- (D) Password Policy

Explanation 16. Correct Answer: C. Disaster Recovery Policy. A Disaster Recovery Policy details the strategy and procedures for recovering IT systems, applications, and data after a catastrophic event. Defining Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) like in this scenario are essential components of this policy.

Option A is incorrect. Data Retention Policy is about how long data should be stored and when it should be discarded, not how to recover it post-disaster.

Option B is incorrect. An Incident Response Policy is centered around how to handle and respond to security incidents. While related, it does not provide the specifics on recovery objectives and timelines.

Option D is incorrect. Password Policy sets the standards for password creation and management. It doesn't have any direct relevance to disaster recovery processes.

Question 17. A large financial institution is planning to upgrade its IT infrastructure to allow for a more efficient use of hardware resources, faster deployment of applications, and reduced server provisioning times. While evaluating different technologies, which of the following would directly address these needs?

- (A) Network Segmentation
- (B) Intrusion Detection System
- (C) **Virtualization**
- (D) Multi-Factor Authentication

Explanation 17. Correct Answer: C. Virtualization.

Virtualization allows multiple virtual machines to run on a single physical host, maximizing the use of hardware resources. It enables rapid provisioning and deployment of new servers and applications, addressing the requirements of the financial institution.

Option A is incorrect. Network segmentation divides a network into smaller subnetworks, primarily for security and performance reasons. While it's a best practice, it doesn't address the efficient use of hardware or rapid deployment of applications.

Option B is incorrect. An Intrusion Detection System (IDS) monitors and detects malicious activities in a network. While

crucial for security, it doesn't cater to hardware resource efficiency or faster server provisioning.

Option D is incorrect. Multi-Factor Authentication is a security process in which a user provides multiple methods of identification to authenticate their identity. It doesn't impact hardware resource efficiency or application deployment times.

Question 18. Bob receives an email prompting him to verify his identity by clicking on a link. The link directs him to a webpage where he has to provide his username, password, and answer a personal security question. What type of authentication method is being employed here?

- (A) Biometric authentication
- (B) Token-based authentication
- (C) **Two-factor authentication**
- (D) Single sign-on

Explanation 18. Correct Answer: C. Two-factor authentication. Two-factor authentication (2FA) is a security process in which users provide two different authentication factors to verify their identity. In this scenario, Bob is providing something he knows (username and password) and also answering a personal security question, which is another form of "something he knows."

Option A is incorrect. Biometric authentication involves using unique physical or behavioral attributes of a person for verification, such as fingerprints or facial patterns. The scenario doesn't mention any biometric data.

Option B is incorrect. Token-based authentication typically involves using a hardware or software token that generates a time-sensitive code. This was not described in the scenario.

Option D is incorrect. Single sign-on (SSO) allows a user to log in once and gain access to multiple systems without being prompted to log in again for each system. The scenario describes a two-factor authentication process, not SSO.

Question 19. An online banking website employs a system that automatically logs out users after 10 minutes of inactivity to ensure that if a user forgets to log out, no one else can alter the user's banking details. Which principle of the CIA triad is the banking website MOST directly addressing?

- (A) Confidentiality
- (B) Availability
- (C) Authentication
- (D) **Integrity**

Explanation 19. Correct Answer: D. Integrity. The integrity pillar of the CIA triad ensures the accuracy and reliability of data. By logging out users after a period of inactivity, the banking website aims to prevent unauthorized modifications (potentially by someone else who might gain access to the unattended session) to the user's banking details, thereby maintaining the integrity of the data.

Option A is incorrect. While logging out users does have a confidentiality aspect, the primary aim in this scenario is to prevent unauthorized changes rather than unauthorized viewing.

Option B is incorrect. Availability ensures that data and systems are accessible to authorized users when they need it. This scenario doesn't discuss providing or restricting access based on system uptime or accessibility.

Option C is incorrect. Authentication ensures that users are who they claim to be. While the scenario does touch on security measures, the primary concern here is preventing unauthorized changes to data, which aligns with integrity, not authentication.

Question 20. A software development company is looking to migrate its legacy applications to a more modern infrastructure. They want to ensure the applications can be deployed consistently across multiple environments without the challenges of varying dependencies and configurations. Which approach would best achieve this goal?

- (A) Virtual Machine Deployment
- (B) Bare-Metal Deployment
- (C) **Containerization**
- (D) Serverless Computing

Explanation 20. Correct Answer: C. Containerization

Containerization encapsulates an application and its dependencies into a 'container.' This allows the application to be consistently deployed across different environments regardless of variations in configurations or dependencies.

Option A is incorrect. While virtual machines provide an isolated environment for applications, they include the overhead of an entire guest OS and don't directly address the challenge of application dependencies varying across environments.

Option B is incorrect. Bare-metal deployment involves installing applications directly on hardware without virtualization or containers. This method does not inherently ensure consistent deployment across multiple environments.

Option D is incorrect. Serverless computing abstracts the infrastructure away from the developer, focusing on individual functions. While it provides scalability and simplicity, it doesn't directly address consistent deployment across environments due to dependencies and configurations.

Question 21. Your organization is implementing Infrastructure as Code (IaC) to deploy and manage its cloud infrastructure. As part of a security review, what is a primary concern regarding the use of IaC scripts?

- (A) Lack of graphical interface for infrastructure visualization
- (B) **Hardcoding sensitive data within the scripts**
- (C) Inability to scale the infrastructure dynamically
- (D) Incompatibility with non-cloud environments

Explanation 21. Correct Answer: B. Hardcoding sensitive data within the scripts. Infrastructure as Code (IaC) scripts are meant to automate infrastructure deployment. If sensitive data such as passwords or API keys are hardcoded into these scripts, they could be exposed, leading to potential security breaches. It's essential to use secure methods, like secrets management or encrypted variables, to handle sensitive data.

Option A is incorrect. While IaC focuses on code-driven infrastructure management, many tools provide ways to visualize the infrastructure or are compatible with tools that do.

Option C is incorrect. One of the benefits of IaC is the ability to scale infrastructure dynamically. It allows for automated scaling based on the script or configuration files.

Option D is incorrect. IaC can be used in various environments, not just cloud. It depends on the tool and the platform it supports.

Question 22. A pharmaceutical company is concerned about competitors accessing their formula for a new drug. Which pillar of the CIA triad is MOST directly addressed by their concern?

- (A) Availability
- (B) **Confidentiality**
- (C) Integrity
- (D) Non-repudiation

Explanation 22. Correct Answer: B. Confidentiality. The confidentiality pillar of the CIA triad ensures that information is accessible only to those with authorized access. In this scenario, the company wants to ensure that its drug formula remains secret and is not accessible to unauthorized individuals, particularly competitors.

Option A is incorrect. Availability ensures that information is accessible to authorized users when needed. The concern here is

not about access to the data but rather about preventing unauthorized access.

Option C is incorrect. Integrity ensures the accuracy and reliability of data and systems. The scenario doesn't mention concerns about the formula being altered, only about unauthorized access.

Option D is incorrect. Non-repudiation is a concept ensuring that a party in a dispute cannot deny the authenticity of their actions. It's not directly related to the company's concern about the secrecy of their drug formula.

Question 23. An online gaming platform experiences latency issues during multiplayer sessions, affecting the gameplay experience of its users. The company wants to ensure real-time responsiveness for its players worldwide. Which of the following solutions would BEST mitigate these latency issues?

- (A) **Implementing a Content Delivery Network (CDN)**
- (B) Introducing stricter user authentication methods
- (C) Deploying a centralized database server
- (D) Reducing the game's graphical fidelity

Explanation 23. Correct Answer: A. Implementing a Content Delivery Network (CDN). A CDN involves distributing the hosting of content to multiple locations around the world. For online gaming, this means players can connect to a server closer to their geographic location, thereby reducing latency and improving responsiveness.

Option B is incorrect. While strong authentication methods are crucial for security, they don't address latency or improve the real-time responsiveness of the gaming platform.

Option C is incorrect. Centralizing the database server might actually increase latency for users who are far from the central location.

Option D is incorrect. Reducing graphical fidelity can improve game performance on the client side, but it doesn't address network latency or the real-time responsiveness of multiplayer sessions.

Question 24. A startup company anticipates rapid growth in its user base over the next year. They are considering an architectural model for their application that can handle the projected growth without performance issues. Which of the following would be the BEST design consideration for this situation?

- (A) Implementing strict password policies
- (B) Using a monolithic application design
- (C) Integrating a DDoS protection mechanism
- (D) **Adopting a microservices architecture**

Explanation 24. Correct Answer: D. Adopting a microservices architecture. Microservices architecture breaks down an application into small, independent services that run as separate processes. This allows for better scalability as each service can be scaled individually based on the demand.

Option A is incorrect. While strict password policies are good for security, they don't directly address the scalability concerns of the application architecture.

Option B is incorrect. Monolithic designs are often harder to scale as changes or scaling in one area can affect the entire application.

Option C is incorrect. While DDoS protection is essential for defending against certain types of cyberattacks, it doesn't address the scalability of the application's core architecture.

Question 25. MedGuard, a health tech company, has developed an AI-driven software that predicts potential health risks based on patient data. Before launching in the U.S. market, which of the following industry external considerations should be the company's primary focus?

- (A) Integrating with popular fitness tracking apps in the U.S.
- (B) **Ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA)**
- (C) Surveying U.S. doctors about software interface preferences
- (D) Collaborating with U.S. pharmaceutical companies for promotional deals

Explanation 25. Correct Answer: B. Ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA). HIPAA is a U.S. law designed to provide privacy standards to protect patients' medical records and other health information. For MedGuard, which deals with patient data,

ensuring HIPAA compliance is paramount before launching their software in the U.S. market.

Option A is incorrect. While integration with fitness tracking apps may enhance the software's functionality, the primary concern when dealing with patient data in the U.S. is compliance with HIPAA.

Option C is incorrect. Although feedback from doctors might help improve the software's user interface, the primary industry external consideration should be regulatory compliance, especially when handling sensitive health information.

Option D is incorrect. While partnerships with pharmaceutical companies might be beneficial for marketing or business growth, the primary industry consideration for a health tech company dealing with patient data is ensuring compliance with relevant regulations.

Question 26. An e-commerce company has experienced a Distributed Denial of Service (DDoS) attack, which caused its website to become inaccessible for several hours. To mitigate the impact of such attacks in the future, which of the following would be the BEST corrective control to implement?

(A) Displaying a seal for third-party security certifications on the website

(B) Establishing a Web Application Firewall (WAF) with DDoS protection

(C) Conducting routine vulnerability assessments on the website

(D) Implementing strong password policies for website administrators

Explanation 26. Correct Answer: B. Establishing a Web Application Firewall (WAF) with DDoS protection. A Web Application Firewall (WAF) with DDoS protection can identify and filter out malicious traffic associated with DDoS attacks. As a corrective control, it can help in mitigating the impact and restoring normal service during and after an attack.

Option A is incorrect. Displaying a seal for third-party security certifications on the website acts as a deterrent by showing visitors and potential attackers that the site adheres to security standards. However, it does not mitigate or correct the effects of a DDoS attack.

Option C is incorrect. Conducting routine vulnerability assessments is a detective control that helps in identifying weaknesses. While it's essential for overall security, it doesn't directly correct or mitigate the effects of a DDoS attack.

Option D is incorrect. Implementing strong password policies for website administrators is a preventive control. It ensures that administrators' accounts are secure, but it does not address or correct the issues caused by a DDoS attack.

Question 27. A healthcare organization uses embedded systems in various medical devices. They are aware of the potential threats these systems can pose if not properly secured. Which of the following is NOT a recommended practice when hardening embedded systems in this context?

- (A) Regularly patching and updating the firmware of the devices
- (B) Allowing unrestricted access to the devices for ease of use by the medical staff**
- (C) Disabling unnecessary services and features not required for the device's primary function
- (D) Changing default credentials and using strong, unique passwords for device access

Explanation 27. Correct Answer: B. Allowing unrestricted access to the devices for ease of use by the medical staff.

Unrestricted access can lead to unintentional or deliberate misconfigurations or misuse of the device, compromising its security.

Option A is incorrect. Regularly patching and updating firmware is a critical aspect of maintaining the security of embedded systems, especially with the evolving nature of threats.

Option C is incorrect. Disabling unnecessary services and features reduces the attack surface and is a fundamental principle of system hardening.

Option D is incorrect. Changing default credentials and ensuring strong, unique passwords are in place is essential to prevent unauthorized access.

Question 28. A financial institution wants to ensure that customers are aware of the bank's policies on information sharing and how their personal data is used. Which of the

following security controls would BEST communicate this to customers?

- (A) Implementing end-to-end encryption for online transactions
- (B) **Publishing a privacy policy on the bank's website**
- (C) Conducting annual cybersecurity awareness training for employees
- (D) Using multi-factor authentication for online banking

Explanation 28. Correct Answer: B. Publishing a privacy policy on the bank's website. A privacy policy serves as a directive control as it informs customers about the bank's practices regarding the collection, use, and sharing of their personal data. By reading the policy, customers understand their rights and the bank's responsibilities.

Option A is incorrect. While end-to-end encryption ensures the confidentiality of online transactions, it doesn't inform customers about the bank's policies on information sharing or how their data is used.

Option C is incorrect. Annual cybersecurity awareness training is aimed at employees, not customers. It wouldn't directly communicate the bank's information-sharing policies to its customers.

Option D is incorrect. Using multi-factor authentication improves the security of online banking by requiring multiple forms of verification. However, it doesn't communicate to customers how their personal data is used or the bank's information-sharing policies.

Question 29. A company detected a DDoS attack that lasted for several weeks. The attackers used a botnet of millions of infected devices and frequently rotated attack vectors to bypass mitigation efforts. This prolonged and resource-intensive attack suggests which kind of threat actor's resources and funding?

- (A) Amateur hacker with minimal resources
- (B) Cybersecurity researcher testing vulnerabilities
- (C) Nation-state actor with strategic interests
- (D) **Organized crime syndicate with substantial funding**

Explanation 29. Correct Answer: D. Organized crime syndicate with substantial funding. The scale and duration of the DDoS attack, combined with the use of a massive botnet and frequent rotation of attack vectors, point to a threat actor with significant resources. While nation-states could conduct such attacks, DDoS campaigns are also a hallmark of well-funded organized crime syndicates, especially when financial or strategic extortion could be a motive.

Option A is incorrect. An amateur hacker with minimal resources would not have the capability to sustain a large-scale DDoS attack using a botnet of millions of devices over several weeks.

Option B is incorrect. Cybersecurity researchers typically do not engage in malicious activities, and launching a prolonged DDoS attack would be unethical and illegal.

Option C is incorrect. While a nation-state actor might have the resources to launch such an attack, DDoS attacks, especially

those of extortion nature, are more commonly associated with organized crime syndicates.

Question 30. AlphaCorp is migrating to cloud infrastructure and wants to ensure all virtual machines (VMs) are securely configured from the onset. Before deploying multiple VM instances, what should AlphaCorp do to ensure each VM starts from a secure configuration?

- (A) Use the default VM templates provided by the cloud provider
- (B) Establish a secure baseline for VM configurations and use it for deployment**
- (C) Regularly backup all VMs
- (D) Use multi-factor authentication for cloud access

Explanation 30. Correct Answer: B. Establish a secure baseline for VM configurations and use it for deployment.

Establishing a secure baseline for VM configurations ensures that each VM is deployed with a set of standard security settings, reducing vulnerabilities from default configurations or potential misconfigurations.

Option A is incorrect. Relying solely on default VM templates provided by cloud providers may not meet the specific security requirements of an organization. Customizing and creating a secure baseline is more effective.

Option C is incorrect. While regular backups are essential for data recovery, they do not directly ensure that VMs start from a secure configuration.

Option D is incorrect. Multi-factor authentication is a crucial security measure for accessing cloud resources, but it doesn't ensure that VMs are deployed with secure configurations.

Question 31. SecureNet Ltd. wants to protect user accounts from brute force attacks. They want to implement a measure where, after a certain number of failed login attempts, the account would become temporarily inaccessible. Which standard best suits this requirement?

- (A) Password minimum length
- (B) **Account lockout threshold**
- (C) Mandatory password resets
- (D) Two-factor authentication

Explanation 31. Correct Answer: B. Account lockout threshold. The account lockout threshold defines the number of consecutive failed login attempts after which a user account is locked out, preventing further attempts for a specified duration. This measure directly deters brute force attacks by making rapid, repeated login attempts unfeasible.

Option A is incorrect. Password minimum length dictates how long a password must be, which can deter certain brute force attempts but doesn't address the rapid, repeated attempts characteristic of such attacks.

Option C is incorrect. Mandatory password resets force users to change their passwords at regular intervals. While this might protect against the use of older stolen credentials, it doesn't prevent brute force attacks.

Option D is incorrect. Two-factor authentication requires two forms of identification to access an account. Although it significantly enhances security, it doesn't limit login attempts based on failed attempts.

Question 32. An energy company is looking to enhance the security of its ICS/SCADA systems. They have realized that default configurations might have vulnerabilities. Which of the following is the BEST initial step to take in securing their ICS/SCADA systems?

- (A) Connect the ICS/SCADA systems to the internet for remote monitoring
- (B) Use commercial off-the-shelf software to add a layer of security
- (C) **Implement a secure baseline configuration tailored to the ICS/SCADA environment**
- (D) Increase the number of users with administrative privileges to ensure rapid response to issues

Explanation 32. Correct Answer: C. Implement a secure baseline configuration tailored to the ICS/SCADA environment. Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems are critical in managing industrial processes. Implementing a secure baseline configuration tailored to these systems ensures that unnecessary services and potential vulnerabilities are minimized.

Option A is incorrect. Connecting ICS/SCADA systems directly to the internet exposes them to a wide range of threats and potential cyber-attacks.

Option B is incorrect. While commercial off-the-shelf software can be beneficial, it's not the best initial step. Secure baselines tailored to the ICS/SCADA environment are more effective.

Option D is incorrect. Increasing the number of users with administrative privileges contradicts the principle of least privilege and can introduce more security vulnerabilities.

Question 33. The IT department wants to monitor network traffic in real time to detect any anomalies or malicious activities. Which of the following security controls can accomplish this?

- (A) Security policy documentation
- (B) **Intrusion Detection System (IDS)**
- (C) Employee code of conduct
- (D) Access Control Lists (ACL)

Explanation 33. Correct Answer: B. Intrusion Detection System (IDS). An Intrusion Detection System (IDS) is a technical control that monitors network traffic in real-time and alerts administrators to any suspicious or malicious activities based on predefined rules or heuristics.

Option A is incorrect. Security policy documentation is an administrative control. It provides guidelines and procedures for maintaining security but does not actively monitor network traffic.

Option C is incorrect. Employee code of conduct is an administrative control. It provides guidelines on how employees

should behave in a professional setting but does not actively monitor network traffic.

Option D is incorrect. Access Control Lists (ACL) are technical controls, but they are used to define permissions on who can access specific resources. They do not actively monitor network traffic in real-time for anomalies or malicious activities.

Question 34. A company is located in an area prone to natural disasters such as earthquakes and floods. Which of the following physical security controls would be MOST effective in ensuring the safety of the company's IT infrastructure?

- (A) Using biometric authentication for server access
- (B) Deploying a firewall to protect against cyber threats
- (C) **Establishing a raised floor system in the data center**
- (D) Conducting penetration testing on a regular basis

Explanation 34. Correct Answer: C. Establishing a raised floor system in the data center. A raised floor system in a data center serves as a physical control by elevating equipment off the ground, helping to protect it from potential water damage in the event of flooding and providing some protection from other environmental risks.

Option A is incorrect. Using biometric authentication is a technical control that enhances security by confirming users' identities based on physical or behavioral attributes. While it strengthens access security, it doesn't provide protection against natural disasters.

Option B is incorrect. Deploying a firewall is a technical control that guards against unauthorized access to or from a private network. While it protects against cyber threats, it doesn't offer protection against physical threats like natural disasters.

Option D is incorrect. Conducting penetration testing is a technical and sometimes operational control that identifies vulnerabilities in an organization's digital assets. While it enhances cyber security, it doesn't protect infrastructure against physical threats.

Question 35. A network engineer is preparing a new batch of routers for deployment in a large organization. Which of the following steps should the engineer prioritize to ensure that the routers are securely configured from the start?

- (A) Configure the routers to use DHCP to dynamically assign IP addresses to connected devices
- (B) Change the default administrative credentials on the routers**
- (C) Update the routers' firmware to the latest, most feature-rich version, regardless of its security posture
- (D) Customize the routers' LED colors for easy identification in the server room

Explanation 35. Correct Answer: B. Change the default administrative credentials on the routers. Routers often come with default credentials that are widely known and can be easily exploited by attackers. Changing these credentials is essential for establishing a secure baseline.

Option A is incorrect. While DHCP is commonly used in many networks, enabling it is not necessarily a secure baseline action. Additionally, DHCP on routers can be exploited if not securely configured.

Option C is incorrect. Blindly updating to the latest firmware without considering its security posture can introduce vulnerabilities. It's important to ensure that the firmware is both updated and secure.

Option D is incorrect. Customizing LED colors relates to physical identification and does not inherently improve the security configuration of a router.

Question 36. SecureCom, a telecommunications company, is planning to expand its infrastructure across Country A. The nation recently updated its telecommunications regulations and mandates strict guidelines for all external communications. Which of the following should be SecureCom's primary focus as it begins its expansion?

- (A) Increasing advertising budget to gain a stronger market presence in Country A
- (B) **Ensuring its infrastructure meets the national standards for secure and encrypted communications**
- (C) Collaborating with local tech companies to better understand the culture of Country A
- (D) Launching new products tailored to the preferences of Country A's residents

Explanation 36. Correct Answer: B. Ensuring its infrastructure meets the national standards for secure and

encrypted communications. Telecommunication companies, by their nature, handle vast amounts of data and communication traffic. As such, when a nation mandates specific security guidelines for external communications, companies like SecureCom must ensure their infrastructure complies with those guidelines to avoid legal and financial repercussions.

Option A is incorrect. While advertising is essential for market growth, the primary concern when expanding infrastructure in a country with strict telecommunications regulations should be compliance.

Option C is incorrect. Collaborating with local tech companies can offer insights into the local market, but regulatory compliance should remain the primary focus, especially given the updated regulations.

Option D is incorrect. Launching tailored products is a sound business strategy, but without ensuring compliance with national regulations, the company might face significant challenges.

Question 37. A medical company has recently deployed a device to monitor patient heart rates in real time. This device uses a real-time operating system (RTOS) to guarantee immediate response times. The security team is concerned about potential risks. Which of the following would be a KEY recommendation to enhance the security of such devices?

- (A) Ensure real-time data analysis capabilities
- (B) Integrate the device with the corporate cloud for backups

- (C) **Implement strict network segmentation for the device**
- (D) Increase the storage capacity of the device

Explanation 37. Correct Answer: C. Implement strict network segmentation for the device. To protect RTOS devices, which often prioritize performance over security, it's crucial to minimize their exposure to potential threats. By segmenting the network, you can isolate the device from other systems and reduce the risk of a security incident.

Option A is incorrect. Real-time data analysis is more about performance and functionality than security.

Option B is incorrect. Integrating the device with the corporate cloud could introduce more security concerns, especially if the cloud environment is not secured properly.

Option D is incorrect. Storage capacity is a matter of device functionality, not a direct security enhancement for an RTOS device.

Question 38. DigitalZone Corp, a marketing company, collects personal data from users and determines how and why that data will be processed. At the same time, they engage an external company, CloudSolutions, to store and manage this data. In this scenario, what role does DigitalZone Corp play in relation to data protection regulations?

- (A) Processor
- (B) Data subject

- (C) **Controller**
- (D) Third-party provider

Explanation 38. Correct Answer: C. Controller. DigitalZone Corp makes decisions about how and why the data is processed, which means they play the role of the controller in the context of data protection regulations.

Option A is incorrect. The processor is the entity that processes personal data on behalf of the controller. In this scenario, CloudSolutions acts as the processor as they are storing and managing the data for DigitalZone Corp.

Option B is incorrect. The data subject is the individual whose personal data is being collected. It's not an entity that makes decisions about the data or processes it.

Option D is incorrect. While CloudSolutions could be considered a third-party provider, this term is broader and does not specifically refer to an entity's role in data protection terms as a controller or processor.

Question 39. During an annual review, a company discovered that one of its critical systems had several unscheduled downtimes over the year. The CTO has recommended a move towards high availability architecture to address this. What is the PRIMARY concern when implementing high availability?

- (A) **Ensuring that there are no single points of failure**
- (B) Ensuring that the system is patched regularly
- (C) Implementing multi-factor authentication
- (D) Storing backups in multiple geographical locations

Explanation 39. Correct Answer: A. Ensuring that there are no single points of failure. In a high availability (HA) system, eliminating single points of failure is of utmost importance. By ensuring redundancy at every potential failure point, the system can remain operational even if a component fails.

Option B is incorrect. While patching is important for security, it is not the primary concern when implementing high availability.

Option C is incorrect. Multi-factor authentication is essential for secure access but does not directly relate to high availability architecture.

Option D is incorrect. Having backups in various geographical locations is more relevant to disaster recovery than to high availability.

Question 40. In a cloud environment, which of the following matrices defines the shared responsibilities between the cloud provider and the customer for specific cloud service models?

- (A) Shared Accountability Matrix
- (B) Cloud Resource Allocation Table
- (C) Cloud Security Posture Matrix
- (D) **Cloud Responsibility Matrix**

Explanation 40. Correct Answer: D. Cloud Responsibility Matrix. The Cloud Responsibility Matrix defines the shared responsibilities between the cloud provider and the customer in a cloud environment, delineating what security measures the

provider will handle and which ones are the responsibility of the customer.

Option A is incorrect. While the term “Shared Accountability Matrix” may sound relevant, there’s no standard matrix in cloud computing with this name. Shared responsibility is the concept, but the actual term used in the context of cloud security is the “Cloud Responsibility Matrix.”

Option B is incorrect. A “Cloud Resource Allocation Table” is not a standard term associated with delineating responsibilities in the cloud. It sounds more related to how resources, such as compute or storage, might be allocated.

Option C is incorrect. “Cloud Security Posture Matrix” is not a recognized term for defining shared responsibilities in cloud environments. Instead, it sounds more like a potential term for an organization’s stance or positioning regarding cloud security.

Question 41. A multinational company is planning to issue company-owned mobile devices to its executives. Given the sensitivity of the data the executives handle, what hardening measure would be MOST effective to ensure the security of these mobile devices?

- (A) Regularly updating the company's social media profiles to mention the security measures taken
- (B) **Implementing biometric authentication in addition to strong passcodes**
- (C) Turning off Bluetooth and Wi-Fi when not in use
- (D) Setting the devices to display brighter screen colors

Explanation 41. Correct Answer: B. Implementing biometric authentication in addition to strong passcodes.

Biometric authentication (like fingerprint or facial recognition) combined with strong passcodes provides a robust multi-factor authentication mechanism, making unauthorized access to the device significantly more challenging.

Option A is incorrect. Publicly announcing security measures on social media does not harden the device. Moreover, divulging too much about security practices could expose the organization to targeted attacks.

Option C is incorrect. While turning off Bluetooth and Wi-Fi can reduce certain attack vectors, it's not as comprehensive a security measure as implementing strong multi-factor authentication.

Option D is incorrect. Screen colors have no direct correlation to the security hardening of a device.

Question 42. A multinational company is deploying a new set of servers in its data centers across various countries. Which of the following steps should be taken FIRST to ensure the servers are secured against potential threats?

- (A) Set up a monitoring system to alert the IT team of any irregular activities
- (B) Deploy all the software applications the company might need in the future
- (C) Use the server's default configuration to ensure manufacturer's best practices are maintained

(D) Disable any unused services and ports on the server

Explanation 42. Correct Answer: D. Disable any unused services and ports on the server. When setting up a new server, it's crucial to minimize its attack surface. Disabling unused services and ports ensures that only necessary services run on the server, reducing potential vulnerabilities.

Option A is incorrect. While monitoring is vital for security, before setting up a monitoring system, it's more crucial to harden the server to minimize vulnerabilities. Monitoring should complement hardening measures.

Option B is incorrect. Deploying all the software applications the company might need in the future can introduce unnecessary vulnerabilities and overhead. It's better to install only what's needed and keep the server lean.

Option C is incorrect. Relying on a server's default configuration can be risky, as it might not be tailored for an organization's specific needs and could have open ports or services that are unnecessary.

Question 43. During an incident response, the IT team discovers malware that collects information about military projects. The malware sends the data to a server located in a foreign country. Which type of threat actor would MOST likely be involved in this type of cyber espionage?

- (A) Disgruntled employee**
- (B) Nation-state**

- (C) Phishing scam artist
- (D) Hacktivist

Explanation 43. Correct Answer: B. Nation-state. Malware that specifically targets information about military projects and sends data to a foreign server is indicative of cyber espionage, a tactic commonly employed by nation-states. They have the motivation to gather intelligence and potentially disrupt or gain advantages over other nations, particularly concerning military or defense-related data.

Option A is incorrect. While a disgruntled employee might have a motive to harm the company, they wouldn't typically be involved in the collection of military project information for a foreign nation.

Option C is incorrect. Phishing scam artists primarily focus on deceiving individuals into revealing personal or financial information. They typically don't have interest or resources for collecting military-specific data for foreign espionage.

Option D is incorrect. Hacktivists are typically motivated by ideological, environmental, or political causes. While they might disrupt services or leak information, targeting military projects for a foreign nation isn't a typical characteristic of their activities.

Question 44. A large e-commerce platform is facing challenges during peak sale periods, where the influx of users causes slowdowns and occasional outages. Which of the following solutions would BEST improve scalability during these high-

demand times?

- (A) Implement a centralized logging system
- (B) **Employ auto-scaling cloud solutions**
- (C) Increase the frequency of data backups
- (D) Mandate regular security training for employees

Explanation 44. Correct Answer: B. Employ auto-scaling cloud solutions. Auto-scaling in cloud solutions automatically adjusts the number of computational resources based on the actual demand. During peak periods, resources can be automatically increased to handle the demand, ensuring the system remains scalable and responsive.

Option A is incorrect. A centralized logging system is beneficial for monitoring and troubleshooting, but it does not directly address scalability during peak times.

Option C is incorrect. Increasing the frequency of data backups is a good practice for data integrity and recovery but does not handle scalability concerns directly.

Option D is incorrect. Regular security training is crucial for a company's cybersecurity posture, but it does not address the architectural scalability of the platform.

Question 45. A large enterprise is considering a transition to a more flexible and programmable network architecture. They want to centralize the control plane, allowing for automated, programmable network configurations and rapid provisioning. Which network architecture model should they consider?

- (A) VLAN (Virtual Local Area Network)

- (B) MPLS (Multiprotocol Label Switching)
- (C) VPN (Virtual Private Network)
- (D) **SDN (Software-Defined Networking)**

Explanation 45. Correct Answer: D. SDN (Software-Defined Networking). Software-Defined Networking (SDN) centralizes the control plane, decoupling it from the data plane. This allows for a more flexible and programmable network, enabling automated configurations, and rapid provisioning.

Option A is incorrect. A VLAN is used to create logical networks within a physical network but doesn't provide centralized control or programmability across the entire network.

Option B is incorrect. MPLS is a type of data-carrying technique for high-performance telecommunications networks. It doesn't centralize network control or enhance programmability as SDN does.

Option C is incorrect. A VPN is designed to provide a secure tunnel between networks over potentially insecure mediums like the internet. It does not offer the centralized, programmable configuration benefits of SDN.

Question 46. An audit report indicates that several network switches in a data center lack security configurations, making them potential targets for attackers. Which of the following hardening techniques would BEST reduce the risk associated with these switches?

- (A) Configuring port mirroring to monitor network traffic

- (B) **Disabling unused switch ports**
- (C) Implementing load balancing across the switches
- (D) Increasing the MAC address table size for performance

Explanation 46. Correct Answer: B. Disabling unused switch ports. By disabling unused switch ports, you minimize potential points of entry for unauthorized devices or attackers. This is a basic step in network switch hardening.

Option A is incorrect. Port mirroring is used for monitoring and isn't directly a hardening technique. While monitoring is crucial for security, it doesn't necessarily prevent unauthorized access.

Option C is incorrect. Load balancing is primarily about distributing network traffic efficiently across multiple paths or resources, and it doesn't inherently harden the switches.

Option D is incorrect. Increasing the MAC address table size might improve switch performance in certain scenarios, but it does not harden the switch against potential security threats.

Question 47. An e-commerce platform reported a series of breaches over the past month. With each breach, financial and personal data of thousands of users were exfiltrated. The perpetrators subsequently sold the data on the dark web. Which type of threat actor is MOST likely behind these breaches?

- (A) Insider threat
- (B) Hacktivist

- (C) **Organized crime syndicate**
- (D) Nation-state

Explanation 47. Correct Answer: C. Organized crime syndicate. Organized crime syndicates are primarily motivated by financial gains. The act of exfiltrating financial and personal data from an e-commerce platform, only to sell it on the dark web, aligns with the profit-driven motives of organized crime groups.

Option A is incorrect. While insider threats can indeed pose significant risks, they are typically motivated by personal grievances, revenge, or opportunistic financial gains. The systematic breaches and subsequent sale of data on the dark web point more towards an organized group than an individual insider.

Option B is incorrect. Hacktivists primarily target organizations to further or protest a political or social cause. The described actions, focused on profiting from stolen data, are not aligned with typical hacktivist motives.

Option D is incorrect. While nation-states might engage in cyber espionage or cyber warfare for political or strategic reasons, they are not typically involved in the theft of financial data for direct monetary gain.

Question 48. A company's primary security control for accessing secure server rooms is a biometric fingerprint scanner. However, the scanner occasionally malfunctions in high humidity. The security team is considering an alternative

solution to grant access when the primary method fails. Which of the following would be the MOST appropriate compensating control?

- (A) **Implementing a security token-based authentication system**
- (B) Employing security guards at the main entrance
- (C) Installing security cameras inside the server room
- (D) Conducting regular server room audits

Explanation 48. Correct Answer: A. Implementing a security token-based authentication system. A security token-based authentication system would act as an alternative method for verifying the identity of individuals when the primary control (biometric fingerprint scanner) fails. This serves as a direct compensating control for access.

Option B is incorrect. While security guards at the main entrance can provide an added layer of security, they aren't a direct compensating control for a malfunctioning biometric system in a specific location like the server room.

Option C is incorrect. While security cameras provide surveillance, they don't act as an alternative method for granting or denying access to the server room.

Option D is incorrect. Conducting regular server room audits is a detective control. It won't provide real-time access or compensate for the malfunctioning fingerprint scanner.

Question 49. A medium-sized financial firm has noticed a series of unauthorized transactions moving funds from

legitimate accounts to overseas locations. After investigating, it was found that a group was responsible for exploiting vulnerabilities in the firm's transaction system. Which of the following motivations is most likely driving this group's actions?

- (A) Seeking notoriety within the hacker community
- (B) **Financial gain from unauthorized transactions**
- (C) Demonstrating political beliefs against financial institutions
- (D) Espionage to uncover the firm's investment strategies

Explanation 49. Correct Answer: B. Financial gain from unauthorized transactions. The unauthorized transactions moving funds to overseas locations indicate a direct attempt to illicitly acquire funds, pointing towards a motivation of financial gain.

Option A is incorrect. There's no evidence to suggest the group's actions are driven by a desire for recognition or notoriety. The focus is on moving funds.

Option C is incorrect. While some groups might target financial institutions to make a political statement, the unauthorized transactions to overseas accounts suggest a financial motive, not a political one.

Option D is incorrect. There's no indication the group is interested in the firm's investment strategies. The activity is focused on moving money, not gathering intelligence.

Question 50. TechGuard Corp. conducts a risk assessment every six months to identify new vulnerabilities and ensure that previous risk-mitigation strategies remain effective. This type of risk assessment is best described as:

- (A) Periodic
- (B) Ad hoc
- (C) Continuous
- (D) **Recurring**

Explanation 50. Correct Answer: D. Recurring. Recurring risk assessments are those that are conducted at regular intervals, such as quarterly, biannually, or annually, to continually identify, review, and address vulnerabilities and threats.

Option A is incorrect. While “periodic” might sound similar to “recurring”, in the context of risk assessments, the term “recurring” more accurately describes assessments that are conducted regularly at defined intervals.

Option B is incorrect. Ad hoc risk assessments are done in response to a specific event or situation and are not planned in advance.

Option C is incorrect. Continuous risk assessments involve constant or ongoing monitoring of risks, rather than taking place at set intervals.

Question 51. An e-commerce company recently faced a DDoS attack that rendered its website unavailable for several hours. While reflecting on the incident, the CISO emphasized the

importance of having a detailed plan that includes identification, containment, eradication, recovery, and lessons learned. Which policy primarily encompasses these stages for handling security incidents?

- (A) Change Management Policy
- (B) **Incident Response Policy**
- (C) Disaster Recovery Policy
- (D) Remote Access Policy

Explanation 51. Correct Answer: B. Incident Response Policy. An Incident Response Policy outlines the procedures and guidelines for effectively responding to and managing security incidents. It includes various stages like identification, containment, eradication, recovery, and lessons learned to ensure a systematic approach to handling security threats.

Option A is incorrect. A Change Management Policy focuses on procedures and guidelines for making changes in the IT environment to ensure stability and security. It does not deal with responding to security incidents directly.

Option C is incorrect. The Disaster Recovery Policy pertains to recovering IT systems, applications, and data after a catastrophic event, rather than the steps for managing security incidents.

Option D is incorrect. Remote Access Policy details the guidelines for accessing the organization's network from remote locations. It doesn't provide a structured methodology for handling security incidents.

Question 52. MatrixCorp recently adopted a mobile strategy where employees are provided with company-owned devices. These devices are also allowed for personal use, but the organization retains the ability to manage and monitor them. Which deployment model is MatrixCorp using?

- (A) Bring Your Own Device (BYOD)
- (B) Choose Your Own Device (CYOD)
- (C) **Corporate-owned, Personally Enabled (COPE)**
- (D) Public Device Deployment (PDD)

Explanation 52. Correct Answer: C. Corporate-owned, Personally Enabled (COPE). The COPE model involves organizations providing employees with company-owned devices that they can also use for personal tasks. However, the company retains full control, management, and monitoring capabilities over these devices.

Option A is incorrect. In the BYOD model, employees use their personal devices for work, not company-provided ones.

Option B is incorrect. CYOD allows employees to select a device from a list of company-approved devices, but the emphasis is on choice rather than personal use of corporate-owned devices.

Option D is incorrect. Public Device Deployment (PDD) is not a recognized deployment model in the context of mobile solutions.

Question 53. The network administrator of a rapidly growing tech firm is concerned about the potential vulnerabilities of the

company's switches. Which of the following measures is MOST effective in hardening these network switches against possible attacks?

- (A) Assigning static IP addresses to all connected devices
- (B) **Implementing strong password policies for switch access**
- (C) Upgrading the switches to support 10Gbps for future expansion
- (D) Customizing the switch LED colors for easy identification

Explanation 53. Correct Answer: B. Implementing strong password policies for switch access. Hardening switches involves reducing their vulnerability to unauthorized access and potential misuse. Implementing strong password policies ensures that only authorized personnel can access and configure the switches.

Option A is incorrect. While assigning static IP addresses might help in network management, it does not inherently harden a switch against potential attacks.

Option C is incorrect. Upgrading the speed capabilities of switches, such as supporting 10Gbps, is a performance enhancement and not directly related to hardening or security.

Option D is incorrect. Customizing LED colors is related to physical identification and does not improve the security posture of the switch.

Question 54. A developer at your company is excited about the scalability benefits of serverless architecture and has deployed a new service using it. However, you notice an increased bill due to the service even when it's not in use. Which of the following could be a contributing factor?

- (A) **The serverless functions are continuously triggered by unintended events**
- (B) The server hardware is outdated
- (C) The load balancer is misconfigured
- (D) The organization lacks a Content Delivery Network (CDN)

Explanation 54. Correct Answer: A. The serverless functions are continuously triggered by unintended events. Serverless architectures charge based on the number of function invocations and the execution time. If there are unintended events, such as rogue requests or misconfigured triggers, continuously invoking the serverless functions, it could lead to unexpected costs.

Option B is incorrect. In a serverless architecture, the responsibility of server hardware management lies with the service provider. The customer is abstracted from the hardware details.

Option C is incorrect. A misconfigured load balancer might affect availability or performance but is not directly related to unexpected cost hikes in a serverless deployment.

Option D is incorrect. While CDNs are valuable for optimizing content delivery, they are not directly related to the cost

implications of unintended function invocations in a serverless architecture.

Question 55. AlphaTech wants to ensure that its remote employees follow best security practices when working from home. The security team has been tasked with drafting a set of guidelines for remote work. What should be the primary focus of these guidelines?

- (A) Outlining punitive measures for non-compliance
- (B) Stating the company's legal position on remote work
- (C) **Recommending security measures for home networks and devices**
- (D) Dictating the exact software and hardware specifications for remote workers

Explanation 55. Correct Answer: C. Recommending security measures for home networks and devices.

Guidelines aim to provide advice and recommendations. In the context of remote work, they would suggest best security practices for securing home networks and devices without being overly prescriptive.

Option A is incorrect. Punitive measures and compliance repercussions are typically outlined in policies or procedures, not guidelines.

Option B is incorrect. The company's legal position on remote work would be part of a policy or a legal document rather than a set of guidelines.

Option D is incorrect. Dictating exact software and hardware specifications would be more in line with standards rather than guidelines. Guidelines would provide broader recommendations.

Question 56. Lisa, a security manager, is reviewing the company's existing policies and realizes that there isn't a comprehensive document detailing the organization's stance, expectations, and commitment to protecting its information assets. Which of the following should Lisa prioritize creating to address this gap?

- (A) Incident Response Plan
- (B) **Information Security Policy**
- (C) Acceptable Use Policy
- (D) Data Backup Strategy

Explanation 56. Correct Answer: B. Information Security Policy. An Information Security Policy is a foundational document that provides a framework for information security throughout the organization. It encompasses the organization's vision, principles, and responsibilities regarding the protection of its data and IT assets.

Option A is incorrect. An Incident Response Plan focuses on the steps to be taken after a security incident has occurred. It does not detail the overall stance of an organization on information security.

Option C is incorrect. An Acceptable Use Policy provides guidelines on how employees should use company resources,

but it doesn't provide a comprehensive overview of an organization's commitment to protecting its information assets.

Option D is incorrect. While a Data Backup Strategy is crucial for data availability and recovery, it does not convey the broader perspective and commitment of the organization to information security.

Question 57. GlobalFin, a fintech company, has developed a new mobile banking application. To avoid any legal complications, which of the following legal external considerations should GlobalFin pay the most attention to before launching the application worldwide?

- (A) Ensuring the app meets global data privacy laws
- (B) Confirming the color scheme aligns with branding regulations in all countries
- (C) Securing copyrights for all images used in the app
- (D) Making sure the app's name isn't offensive in any language

Explanation 57. Correct Answer: A. Ensuring the app meets global data privacy laws. For a mobile banking application, ensuring compliance with global data privacy laws is paramount. Different regions have varying requirements and regulations about how user data should be handled, stored, and processed.

Option B is incorrect. While branding and color schemes are important for marketing, they are not typically subjects of strict legal regulation like data privacy laws.

Option C is incorrect. While securing copyrights is important, the primary legal concern for a banking application would be related to data privacy and security, given the sensitive nature of financial data.

Option D is incorrect. Although it's good practice to ensure an app's name is culturally sensitive, the primary legal concern for a banking app would be data privacy and security regulations.

Question 58. In a microservices architecture, each service should be designed with a specific principle to ensure it performs a specific task and interacts with other services through well-defined interfaces. What principle is this referring to?

- (A) Principle of Least Privilege
- (B) **Single Responsibility Principle**
- (C) Open-Closed Principle
- (D) Zero Trust Model

Explanation 58. Correct Answer: B. Single Responsibility Principle. The Single Responsibility Principle dictates that a class or module (or in the context of microservices, a service) should have only one reason to change, meaning it should only have one job or responsibility. In microservices, this ensures that each service does one thing and does it well, and interacts with others through clear interfaces.

Option A is incorrect. The Principle of Least Privilege is about ensuring that users or services have only the permissions they need to perform their tasks and nothing more. It's not specifically about the design of the service itself.

Option C is incorrect. The Open-Closed Principle is a design principle stating that software entities should be open for extension but closed for modification. While relevant for software design, it's not the primary principle guiding the design of individual microservices.

Option D is incorrect. The Zero Trust Model is a security concept where no one, whether inside or outside the organization, is trusted by default. It's not a principle specific to microservice design.

Question 59. XYZ Corp is in the process of defining clear roles and responsibilities for their IT assets. During a meeting, the team discussed the primary individual who will have the responsibility for the data within a specific IT system and also be the main point of contact for any decisions related to it. Which of the following roles best describes this individual?

- (A) System administrator
- (B) Data custodian
- (C) **System owner**
- (D) End-user

Explanation 59. Correct Answer: C. System owner. The system owner, sometimes known as the data owner, is typically responsible for the data within a specific IT system. They have the primary responsibility for ensuring the confidentiality, integrity, and availability of the data and act as the main point of contact for decisions related to that system.

Option A is incorrect. A system administrator is responsible for the daily management, operations, and support of IT systems

but doesn't usually make high-level decisions about the data contained within them.

Option B is incorrect. A data custodian is typically responsible for implementing the controls and processes as defined by the data owner. They may handle the practical aspects of data management, but they don't usually make overarching decisions about the data.

Option D is incorrect. An end-user utilizes the data or system for their job function but doesn't typically have decision-making responsibilities regarding the data's overall management and protection.

Question 60. An organization with a single physical network infrastructure wants to separate the traffic of its finance department from that of the HR department. They do not want to set up entirely new physical networks but want to ensure that data packets from one department do not mix with the other's. What should the organization implement?

- (A) Air-gapped network
- (B) DMZ (Demilitarized Zone)
- (C) **VLAN (Virtual Local Area Network)**
- (D) VPN (Virtual Private Network)

Explanation 60. Correct Answer: C. VLAN (Virtual Local Area Network). A VLAN allows a network administrator to create a logical network within a physical network. This logical segmentation can separate the traffic of different departments, ensuring that data packets from one VLAN do not mix with another, effectively isolating them.

Option A is incorrect. An air-gapped network is a physically isolated network and would require setting up a new physical network.

Option B is incorrect. A DMZ is a buffer zone between a private network and external networks. It doesn't help in segmenting traffic within the internal network.

Option D is incorrect. A VPN is used to create secure connections over an unsecured network. It does not logically segment traffic within a single physical network.

Question 61. A medium-sized company suffered a data breach. Investigations revealed that an attacker from a rival firm had exploited a misconfigured firewall to gain unauthorized access to the company's database. Based on the attributes of the actor, how would this threat actor be best described?

- (A) Internal actor leveraging physical access
- (B) Internal actor abusing privileges
- (C) External actor using social engineering
- (D) **External actor exploiting technical vulnerabilities**

Explanation 61. Correct Answer: D. External actor exploiting technical vulnerabilities. The attacker originated from outside the victim organization (a rival firm) and exploited a technical issue (misconfigured firewall) to gain access. This categorizes them as an external actor exploiting technical vulnerabilities.

Option A is incorrect. The attacker was from a rival firm and did not utilize physical access within the victim organization. Therefore, this description doesn't match the scenario.

Option B is incorrect. The scenario doesn't mention any internal actors or abuse of privileges. Instead, it describes an external attacker from a rival firm.

Option C is incorrect. While the attacker was external, the scenario does not describe any use of social engineering tactics. Instead, the attacker exploited a technical vulnerability (misconfigured firewall).

Question 62. A global corporation has undergone several IT incidents in the past year, including outages due to natural disasters and cyber attacks. The CEO wants to ensure the organization's IT infrastructure can withstand or rapidly recover from disruptive events. Which of the following best encapsulates this requirement?

- (A) Adopting a Zero Trust Architecture
- (B) Implementing a strict password policy
- (C) **Establishing a Business Continuity Plan (BCP) with emphasis on resilience**
- (D) Regularly updating firewall rules

Explanation 62. Correct Answer: C. Establishing a Business Continuity Plan (BCP) with emphasis on resilience.

Resilience in this context refers to the ability of the IT infrastructure to rapidly recover and continue functioning even after disruptive events. A Business Continuity Plan with a focus

on resilience would help the organization prepare for, respond to, and recover from both natural and man-made incidents.

Option A is incorrect. Zero Trust Architecture emphasizes not trusting any user or system, both inside and outside the perimeter, but it doesn't address resilience against disruptive events directly.

Option B is incorrect. While password policies are essential for security, they are not centered around ensuring resilience against disruptive events.

Option D is incorrect. Updating firewall rules is crucial for keeping out unwanted traffic and potential threats but doesn't directly address the resilience of an IT infrastructure against major disruptive events.

Question 63. A company has faced multiple instances of unauthorized individuals gaining access to their office premises. Which of the following preventive security controls would be MOST effective in preventing unauthorized physical access?

- (A) Implementing a log monitoring solution for network traffic
- (B) Installing video surveillance cameras at all entry and exit points**
- (C) Conducting regular security awareness training for employees
- (D) Implementing a multi-factor authentication system for network access.

Explanation 63. Correct Answer: B. Installing video surveillance cameras at all entry and exit points. Installing video surveillance cameras at all entry and exit points acts as a preventive control by deterring unauthorized individuals from attempting to gain access, given the increased risk of detection and recording.

Option A is incorrect. Implementing a log monitoring solution is a detective control that provides insights into network activities but doesn't prevent unauthorized physical access.

Option C is incorrect. Conducting regular security awareness training is a preventive measure, but its main focus is on making employees aware of security risks and best practices, not directly preventing unauthorized physical access.

Option D is incorrect. Implementing a multi-factor authentication system is a preventive control for unauthorized digital access but doesn't address the prevention of unauthorized physical access.

Question 64. After detecting an unauthorized intrusion into their network, a financial institution wants to implement a control that will restore compromised systems to a known good state. Which of the following would be the MOST appropriate corrective control?

- (A) Implementing Intrusion Detection Systems (IDS) across the network
- (B) Frequently updating firewall rules
- (C) **Restoring systems from verified backups**
- (D) Enabling multi-factor authentication for users

Explanation 64. Correct Answer: C. Deploying infrared (IR) sensors. Infrared (IR) sensors detect infrared radiation, such as the heat emitted by the human body. This makes them particularly effective in detecting human intruders, even in complete darkness, based on the body heat they emit.

Option A is incorrect. While CCTV cameras with LED lights can provide visual surveillance, they rely on light to produce images and may not detect intruders in complete darkness as efficiently as infrared sensors.

Option B is incorrect. Ultrasonic motion sensors detect movement through sound waves, not body heat, making them less efficient in differentiating between a human intruder and other moving objects.

Option D is incorrect. RFID badge readers control access at entry points but do not detect human intruders based on their body heat inside a facility.

Question 65. An organization that processes classified information is implementing a network infrastructure to ensure the highest level of data security. The CISO recommends using a network configuration that ensures the system remains completely disconnected from unsecured networks and any external connections. Which of the following describes this type of configuration?

- (A) DMZ (Demilitarized Zone)
- (B) VPN (Virtual Private Network)
- (C) VLAN (Virtual Local Area Network)
- (D) **Air-gapped network**

Explanation 65. Correct Answer: D. Air-gapped network.

An air-gapped network is a network that is physically isolated from unsecured networks. Computers on an air-gapped network cannot communicate with non-air-gapped computers and aren't connected to external networks or the internet, ensuring the highest level of data security.

Option A is incorrect. A DMZ is a buffer zone between a private network and external networks (typically the internet). It's designed to provide an additional layer of security but does not guarantee complete isolation.

Option B is incorrect. VPNs are used to establish secure connections over an unsecured network, such as the internet. They encrypt the data being transferred but don't physically isolate a network.

Option C is incorrect. A VLAN is a logically segmented network within a physical network. It allows for the separation of broadcast domains in a Layer 2 network, but it doesn't provide complete physical isolation from other networks.

Question 66. A small business detected unauthorized access to its website. The attacker used default login credentials to gain access. What level of sophistication and capability does this attack suggest about the threat actor?

- (A) **Script kiddie with basic skills**
- (B) Expert attacker leveraging advanced techniques
- (C) Nation-state actor with strategic objectives
- (D) Organized crime syndicate targeting high-value assets

Explanation 66. Correct Answer: A. Script kiddie with basic skills. Using default login credentials for unauthorized access typically indicates a low level of sophistication, as this method is basic and requires little to no technical skill. Such attackers, often termed “script kiddies,” usually exploit known vulnerabilities with pre-existing tools or scripts without fully understanding them.

Option B is incorrect. An expert attacker would likely utilize more advanced techniques and not rely solely on default credentials.

Option C is incorrect. While nation-state actors have the capability for sophisticated attacks, the use of default login credentials as the primary method of unauthorized access doesn’t align with the complex methodologies usually employed by such actors.

Option D is incorrect. Organized crime syndicates, especially those targeting high-value assets, would employ more sophisticated techniques than merely using default login credentials.

Question 67. To discourage potential cybercriminals from targeting their online storefront, an e-commerce company is considering various security measures. Which of the following would act MOST effectively as a deterrent control?

(A) Displaying a seal for third-party security certifications on the website

(B) Using a Web Application Firewall (WAF)

- (C) Conducting monthly vulnerability assessments
- (D) Storing customer data in encrypted databases

Explanation 67. Correct Answer: A. Displaying a seal for third-party security certifications on the website. Displaying a seal for third-party security certifications on the website serves as a deterrent control. It sends a message to potential attackers that the site is recognized for its security measures, which can discourage them from attempting an attack.

Option B is incorrect. Using a Web Application Firewall (WAF) is a preventive control. It filters, monitors, and blocks malicious web traffic. While it helps in defending against cyber threats, it doesn't act as a visible deterrent to attackers.

Option C is incorrect. Conducting monthly vulnerability assessments is a detective control. It identifies vulnerabilities to enhance the security posture but doesn't act as a deterrent to potential attackers.

Option D is incorrect. Storing customer data in encrypted databases is a preventive control that ensures unauthorized individuals cannot access or comprehend the stored data. It protects data but doesn't deter potential cybercriminals.

Question 68. A system administrator is setting up an authentication system for a new web application. Which of the following security controls falls under the technical category and ensures that users prove their identity before gaining access?

- (A) Implementing a security awareness training program

- (B) Conducting a background check for new employees
- (C) **Using multi-factor authentication**
- (D) Establishing a clean desk policy

Explanation 68. Correct Answer: C. Using multi-factor authentication. Multi-factor authentication is a technical control that requires users to present two or more pieces of evidence (factors) before gaining access. It provides an additional layer of security to ensure that users are who they say they are.

Option A is incorrect. Implementing a security awareness training program is an administrative control, as it involves educating employees on security best practices rather than using technical measures to enforce them.

Option B is incorrect. Conducting a background check is an administrative control as it involves vetting potential employees before they're hired. This process doesn't directly enforce technical measures on systems or networks.

Option D is incorrect. Establishing a clean desk policy is an administrative control. It sets a guideline for employees to keep their workspaces tidy and free of sensitive information, rather than enforcing technical measures.

Question 69. CyberFirm, a leading software development company, recently updated their server OS due to new features and patches. Given that they have already established and deployed a secure baseline in the past, what should CyberFirm do NEXT to ensure continued security?

- (A) Conduct a complete system reboot for all servers
- (B) Re-deploy the same baseline without any modifications
- (C) Update the secure baseline to include new configurations and then deploy it**
- (D) Implement a new firewall rule for the servers

Explanation 69. Correct Answer: C. Update the secure baseline to include new configurations and then deploy it.

When there are significant updates or changes to systems, it's crucial to review and update the secure baseline accordingly, ensuring it remains relevant and effective for the current environment. After updating the baseline, it should then be re-deployed.

Option A is incorrect. A complete system reboot does not address the maintenance of the secure baseline after an OS update.

Option B is incorrect. Simply re-deploying the same baseline without adjustments might miss out on specific configurations or considerations needed due to the OS update.

Option D is incorrect. While firewall rules are essential for security, they don't directly address the maintenance and updating of a secure baseline.

Question 70. A cybersecurity analyst has noticed a series of sophisticated attacks against critical infrastructure systems in their country. The attacks are highly coordinated, well-funded, and appear to have specific geopolitical objectives. Which type

of threat actor is MOST likely responsible for these attacks?

- (A) Organized crime syndicates
- (B) Script kiddies
- (C) Insider threat
- (D) **Nation-state**

Explanation 70. Correct Answer: D. Nation-state.

Sophisticated, coordinated, and well-funded attacks against national critical infrastructure with clear geopolitical objectives align most closely with the characteristics and motivations of nation-state actors. They often have vast resources and specific political or strategic motives, targeting critical infrastructures to cause significant impact or gain a strategic advantage.

Option A is incorrect. While organized crime syndicates might be well-funded and capable of launching sophisticated attacks, they are typically driven by financial motives rather than geopolitical objectives.

Option B is incorrect. Script kiddies are amateur hackers who use pre-written scripts or tools to exploit vulnerabilities. They typically lack the sophistication and resources to launch coordinated attacks against critical infrastructure.

Option C is incorrect. Insider threats come from individuals within the organization, like employees or contractors. While they can be harmful, the described scenario is more indicative of an external, nation-state actor with significant resources and geopolitical motives.

Question 71. An e-commerce company is preparing for an upcoming Black Friday sale, expecting a surge in web traffic. To ensure their systems remain responsive during the sale, which of the following would be the MOST effective strategy to implement?

- (A) Increasing password complexity for all users
- (B) Limiting the number of products on sale
- (C) **Implementing a content delivery network (CDN)**
- (D) Conducting a yearly security audit

Explanation 71. Correct Answer: C. Implementing a content delivery network (CDN). CDNs distribute the traffic load among multiple servers, often geographically dispersed. This not only speeds up content delivery to users but also helps in handling traffic surges, ensuring the system remains responsive during high-demand periods such as Black Friday sales.

Option A is incorrect. Increasing password complexity can enhance security but does not directly impact system responsiveness during high traffic periods.

Option B is incorrect. Limiting the number of products on sale may reduce server load, but it might also decrease potential revenue and is not a direct method for improving system responsiveness.

Option D is incorrect. While yearly security audits are essential for identifying vulnerabilities, they don't directly address system responsiveness during high traffic periods.

Question 72. Alice wants to access a restricted online portal. The portal asks her to enter a unique username and a secret passphrase only she should know. This process helps the system ensure that Alice is who she claims to be. What security concept is the portal employing?

- (A) Authorization
- (B) Accounting
- (C) Multifactor authentication
- (D) **Authentication**

Explanation 72. Correct Answer: D. Authentication.

Authentication is the process of verifying the identity of a user, system, or application. In the described scenario, Alice is proving her identity to the system by providing a unique username and a passphrase, which are credentials that supposedly only she possesses.

Option A is incorrect. Authorization determines what actions, resources, or services a verified identity is allowed to access or perform. It does not deal with verifying the identity itself.

Option B is incorrect. Accounting involves tracking user activities and recording them for audit purposes. It does not directly verify a user's identity.

Option C is incorrect. Multifactor authentication requires two or more methods of verification from different categories of credentials. The scenario only mentioned a username and passphrase, which is a single-factor authentication method.

Question 73. During a routine check, the IT department discovered that several employees had left their computers on and unattended during lunch break. Which operational security control can help mitigate the risk associated with this behavior?

- (A) Implementing biometric authentication
- (B) Enforcing a strict password policy
- (C) **Deploying an automatic screen lock after inactivity**
- (D) Implementing a secure coding practice

Explanation 73. Correct Answer: C. Deploying an automatic screen lock after inactivity. Deploying an automatic screen lock after a certain period of inactivity is an operational control. It ensures that unattended devices are protected from unauthorized access, thereby mitigating risks associated with employees leaving their computers on and unattended.

Option A is incorrect. Implementing biometric authentication is a technical control. While it enhances security at the point of access, it doesn't ensure that active sessions on unattended devices are secured against unauthorized access.

Option B is incorrect. Enforcing a strict password policy is a managerial control that dictates the creation and use of strong passwords. While it enhances access security, it doesn't secure active sessions on unattended devices.

Option D is incorrect. Implementing a secure coding practice is a technical and sometimes managerial control. It ensures software is written to prevent vulnerabilities but doesn't directly address the risk of unattended computers.

Question 74. A retail company recently suffered a breach where attackers encrypted all point-of-sale systems, rendering them unusable. A ransom note was then received, demanding payment in cryptocurrency to decrypt the systems. What motivation is most evident behind this attack?

- (A) Protesting against the company's environmental policies
- (B) **Financial gain through ransom**
- (C) Espionage to understand the company's supply chain
- (D) Seeking a reputation boost by showing off technical skills

Explanation 74. Correct Answer: B. Financial gain through ransom. The attackers encrypted critical systems and then demanded a ransom to decrypt them. The primary motive in such ransomware attacks is to achieve financial gain by compelling the victim to pay to regain access to their systems.

Option A is incorrect. There's no mention or indication that the attackers were motivated by the company's environmental or any other policies.

Option C is incorrect. There's no evidence suggesting the attackers were interested in the company's supply chain or any other internal information. Their focus was on encryption and ransom.

Option D is incorrect. While demonstrating technical skills might be a byproduct of the attack, the direct demand for payment indicates that financial gain, not notoriety, is the primary motive.

Question 75. In an effort to minimize data breaches from malware, a company is deciding on a control to prevent malicious software from being executed on company devices. Which of the following would be the BEST preventive control?

- (A) Deploying a Network Intrusion Detection System (NIDS)
- (B) Regularly backing up critical data
- (C) **Installing an antivirus software with real-time scanning**
- (D) Performing a forensic analysis after a security incident

Explanation 75. Correct Answer: C. Two-factor authentication. Two-factor authentication (2FA) is a security process in which users provide two different authentication factors to verify their identity. In this scenario, Bob is providing something he knows (username and password) and also answering a personal security question, which is another form of “something he knows.”

Option A is incorrect. Biometric authentication involves using unique physical or behavioral attributes of a person for verification, such as fingerprints or facial patterns. The scenario doesn't mention any biometric data.

Option B is incorrect. Token-based authentication typically involves using a hardware or software token that generates a time-sensitive code. This was not described in the scenario.

Option D is incorrect. Single sign-on (SSO) allows a user to log in once and gain access to multiple systems without being

prompted to log in again for each system. The scenario describes a two-factor authentication process, not SSO.

Question 76. After a recent service outage, a hospital's IT team is reviewing the availability of its patient record system. They want to ensure the system remains operational, even in the event of hardware failures. Which of the following considerations is MOST relevant to this requirement?

- (A) **Implementing database mirroring**
- (B) Regularly updating the system's antivirus definitions
- (C) Using strong encryption for data at rest
- (D) Conducting penetration testing on the system

Explanation 76. Correct Answer: A. Implementing database mirroring. Database mirroring is a solution for increasing the availability of a SQL Server database. Mirroring is implemented on a per-database basis and works only with databases that use the full recovery model. This ensures that in the event of a hardware failure, there's a mirrored copy of the data available.

Option B is incorrect. While updating antivirus definitions is crucial for preventing malware infections, it is not directly related to ensuring high availability in the face of hardware failures.

Option C is incorrect. Encryption is vital for data security but doesn't directly address the high availability needs of a system.

Option D is incorrect. Penetration testing identifies vulnerabilities in the system but doesn't provide a solution for high availability in case of hardware failures.

Question 77. An environmental NGO's website was hacked and replaced with a message decrying their recent campaign against deforestation, claiming they are spreading misinformation. The website was left with a manifesto promoting responsible forestry and sustainable logging practices. Which type of threat actor is MOST likely behind this incident?

- (A) Ransomware gang
- (B) Organized crime syndicate
- (C) **Hactivist**
- (D) Advanced Persistent Threat (APT)

Explanation 77. Correct Answer: C. Hactivist. The attack seems to be motivated by ideological differences regarding deforestation and sustainable logging. Hacktivists typically conduct cyber actions to make political or social statements. The replacement of the NGO's website with a manifesto supports the idea that this is an ideologically motivated attack, typical of hacktivists.

Option A is incorrect. Ransomware gangs primarily focus on encrypting data and demanding payment for its release. There is no mention of a ransom or encrypted data in the described scenario.

Option B is incorrect. Organized crime syndicates are usually motivated by financial gains. The attack on the NGO's website seems to be ideologically driven, not profit-driven.

Option D is incorrect. Advanced Persistent Threats (APTs) are highly organized, often state-sponsored groups that conduct prolonged cyber-espionage campaigns. Their motivations are

typically strategic, political, or espionage-driven. The described attack doesn't fit the profile of an APT operation.

Question 78. A government agency experienced a cyber incident where its communication platforms were breached. The intruders were not interested in extracting sensitive data or causing disruptions but were observed to be silently monitoring diplomatic communications for an extended period. What was the likely motivation of the attackers?

- (A) To gain financial benefits from insider trading
- (B) **Espionage to understand and anticipate diplomatic moves**
- (C) Disgruntlement of an internal employee
- (D) An attempt to expand their cybercriminal network

Explanation 78. Correct Answer: B. Espionage to understand and anticipate diplomatic moves. Silently monitoring diplomatic communications without exfiltrating data or causing disruptions indicates a motivation to understand, anticipate, and potentially manipulate governmental or diplomatic actions. This is a classic example of espionage.

Option A is incorrect. While sensitive information might indeed be valuable for insider trading, the focus on diplomatic communications suggests a broader strategic intent rather than just financial gain.

Option C is incorrect. A disgruntled employee might engage in sabotage or data leakage, but silently monitoring diplomatic communications indicates a higher level of strategy and sophistication usually beyond personal vendettas.

Option D is incorrect. The attackers' actions were specific to monitoring diplomatic channels and did not indicate an attempt to recruit more systems or individuals into a criminal network.

Question 79. During a company's onboarding process, new employees are required to read and acknowledge understanding of various company policies. The HR department wants to ensure that employees are aware of their responsibilities when it comes to the use of company devices and internet resources. Which policy should be included in the onboarding packet to address this?

- (A) Password Complexity Policy
- (B) Data Classification Policy
- (C) **Acceptable Use Policy (AUP)**
- (D) Vendor Management Policy

Explanation 79. Correct Answer: C. Acceptable Use Policy (AUP). The Acceptable Use Policy (AUP) outlines the do's and don'ts for employees regarding the use of company devices, networks, and other IT resources. Including this in the onboarding packet will ensure that new hires are aware of their responsibilities.

Option A is incorrect. While important, the Password Complexity Policy primarily deals with the requirements for creating and managing passwords, not the overall acceptable use of IT resources.

Option B is incorrect. A Data Classification Policy focuses on the categorization of data based on its sensitivity. It doesn't provide guidelines on the acceptable use of IT resources.

Option D is incorrect. The Vendor Management Policy governs the relationship and security expectations between the company and its vendors, not the acceptable use of company IT resources by employees.

Question 80. WhiteCape Healthcare, an international healthcare provider, has a large patient database that includes many EU citizens. They're about to implement a new system to improve data access for physicians. Which of the following regulatory requirements should they pay particular attention to when granting physicians access to EU patient data?

- (A) Ensure data is only accessed for tax reporting purposes
- (B) Acquire explicit consent from patients before sharing data**
- (C) Encrypt all data using a proprietary algorithm
- (D) Store data in a physical server located within the EU

Explanation 80. Correct Answer: B. Acquire explicit consent from patients before sharing data. Under the GDPR, explicit consent from individuals is required before processing or sharing their personal data. This means that EU citizens should have given their clear permission for their data to be accessed and shared.

Option A is incorrect. Accessing data for tax reporting purposes is not directly related to the GDPR's requirement for handling EU citizens' personal healthcare data.

Option C is incorrect. While encryption is a good practice for data protection, GDPR does not mandate using a proprietary

algorithm. Moreover, encryption alone doesn't address the consent requirement.

Option D is incorrect. While the GDPR does have provisions about data transfer outside the EU, simply storing data in a physical server within the EU does not bypass the need for explicit patient consent when sharing their data.

Question 81. An enterprise is deploying IoT-based security cameras across multiple office locations. As the lead security professional, what recommendation would you prioritize to establish a secure baseline for these devices?

(A) Setting the devices to public mode so all employees can access the feed for transparency

(B) **Regularly updating the device firmware to patch known vulnerabilities**

(C) Enabling Universal Plug and Play (UPnP) to ensure easy connectivity for all devices on the network

(D) Using the same password for all cameras for ease of management

Explanation 81. Correct Answer: B. Regularly updating the device firmware to patch known vulnerabilities. Regular firmware updates ensure that the IoT devices are protected against identified vulnerabilities, helping maintain their security posture.

Option A is incorrect. Setting devices to a public mode can lead to potential breaches of privacy and unauthorized access.

Option C is incorrect. UPnP can introduce vulnerabilities by automatically opening ports and allowing devices to set their configurations, potentially leading to security risks.

Option D is incorrect. Using the same password for all devices creates a single point of failure. If one device's password is compromised, all devices become vulnerable.

Question 82. A robotics company is developing an autonomous vehicle that relies on a Real-Time Operating System (RTOS) to manage its operations. The development team wants to ensure that the vehicle's RTOS has a solid security posture. What should the team prioritize when establishing a secure baseline for this RTOS?

- (A) Installing a robust antivirus software
- (B) Enabling all features for maximum functionality
- (C) Regularly backing up the RTOS data to the cloud
- (D) **Minimizing the number of services and open ports**

Explanation 82. Correct Answer: D. Minimizing the number of services and open ports. Reducing the number of services and open ports reduces the attack surface on the RTOS, making it more challenging for attackers to find vulnerabilities.

Option A is incorrect. While antivirus software is essential for many systems, an RTOS, especially one for an autonomous vehicle, would prioritize reducing the attack surface and ensuring real-time performance rather than relying on traditional antivirus solutions.

Option B is incorrect. Enabling all features may introduce unnecessary vulnerabilities. It's best to enable only required functionalities to maintain security.

Option C is incorrect. While backups are crucial for data integrity and recovery, the primary concern for an RTOS, especially in autonomous vehicles, would be real-time performance and reducing potential vulnerabilities.

Question 83. After a recent incident of vandalism, a corporate building is considering implementing security controls that would dissuade potential perpetrators. Which of the following would serve BEST as a deterrent control?

- (A) Encrypting all stored data
- (B) Installing biometric access controls on all entrances
- (C) Implementing regular data backups
- (D) **Placing visible security signage indicating 24/7 surveillance**

Explanation 83. Correct Answer: D. Placing visible security signage indicating 24/7 surveillance. Visible security signage serves as a deterrent control as it discourages potential perpetrators by signaling the risk of detection and consequences, even if actual surveillance might not be active at all times.

Option A is incorrect. Encrypting all stored data is a preventive control that ensures unauthorized individuals cannot access or understand the encrypted information. It doesn't deter acts of physical vandalism.

Option B is incorrect. Installing biometric access controls is a preventive control that restricts physical access based on unique biological attributes. While it prevents unauthorized access, it doesn't act as a visible deterrent to vandalism or other potential threats.

Option C is incorrect. Implementing regular data backups is a corrective control designed to restore data after a security incident. It doesn't deter potential threats.

Question 84. The finance department of a global corporation found a series of unauthorized transactions originating from an employee's workstation. Investigations revealed that the employee had been bypassing company policies to make unauthorized investments using company funds. Based on the attributes of the actor, how can this threat actor be best categorized?

- (A) External actor leveraging malware
- (B) External actor exploiting vulnerabilities
- (C) **Internal actor with direct access**
- (D) Internal actor with indirect access

Explanation 84. Correct Answer: C. Internal actor with direct access. The threat originated from an employee's workstation within the organization, making it an internal threat. Since the employee used their own workstation and credentials to make unauthorized transactions, they had direct access, categorizing them as an internal actor with direct access.

Option A is incorrect. There's no mention of malware being used in this scenario, and the unauthorized transactions came

from an employee's workstation, indicating an internal rather than external threat.

Option B is incorrect. The scenario doesn't describe an external actor exploiting vulnerabilities. Instead, it describes an employee making unauthorized transactions from within the organization.

Option D is incorrect. The employee in this scenario had direct access to the company's resources, as they used their own workstation and credentials. Thus, they aren't categorized as having indirect access.

Question 85. After a series of cyberattacks, BetaTech, a financial institution, decided to standardize the configurations across its entire server fleet. They've established a secure baseline configuration for their servers. What should be the NEXT step in ensuring the servers conform to this new baseline?

- (A) Frequently conduct vulnerability scanning on all servers
- (B) Introduce biometric authentication for server access
- (C) **Deploy the secure baseline across all servers**
- (D) Monitor network traffic to detect anomalies

Explanation 85. Correct Answer: C. Deploy the secure baseline across all servers. After establishing a secure baseline, the immediate next step is to deploy or apply this baseline to the servers. This ensures that all servers start from a standardized and secure configuration.

Option A is incorrect. While vulnerability scanning is crucial, it is more of a continuous process to identify potential vulnerabilities and doesn't directly apply the secure baseline to the servers.

Option B is incorrect. Biometric authentication, though a valuable security measure, does not address the deployment of the established secure baseline on servers.

Option D is incorrect. Monitoring network traffic is essential for detecting potential threats, but it does not directly ensure the deployment of the secure baseline on servers.

Question 86. ClearView Industries wants to give their employees the flexibility to choose their own devices for work while retaining control over the device configurations and applications. Which deployment model would be the MOST appropriate for ClearView's objectives?

- (A) Bring Your Own Device (BYOD)
- (B) **Choose Your Own Device (CYOD)**
- (C) Corporate-owned, Personally Enabled (COPE)
- (D) Fixed Device Deployment (FDD)

Explanation 86. Correct Answer: B. Choose Your Own Device (CYOD). In the CYOD model, employees are allowed to choose a device from a list of approved devices. The organization retains control over the device configurations and applications, ensuring a blend of user preference and corporate security.

Option A is incorrect. BYOD allows employees to bring their personal devices to work, which means the organization has less control over the configurations and applications.

Option C is incorrect. While COPE provides devices owned by the corporation and allows personal use, it does not necessarily offer employees the choice of which device they get.

Option D is incorrect. Fixed Device Deployment (FDD) is not a standard deployment model in the context of mobile solutions, and it does not reflect the flexibility of device choice.

Question 87. XYZ Company uses MDM to manage company-owned and employee-owned mobile devices. An employee reported losing their personal phone over the weekend. What MDM feature should the IT department use to ensure that sensitive company data on the lost phone isn't accessed?

- (A) Monitor the device's location
- (B) Force update the device's apps
- (C) **Remote wipe the device**
- (D) Change the user's email password

Explanation 87. Correct Answer: C. Remote wipe the device. Using the remote wipe feature, the IT department can erase all data, including company data, from the lost device, ensuring that sensitive information doesn't fall into the wrong hands.

Option A is incorrect. Monitoring the device's location might help in finding it but doesn't prevent unauthorized access to the data on the device.

Option B is incorrect. Force updating the device's apps might address vulnerabilities in the apps but doesn't directly protect the company data on the device.

Option D is incorrect. Changing the user's email password can prevent unauthorized access to the user's email, but it doesn't secure other sensitive company data that might be on the device.

Question 88. During a major sports event, a broadcasting company's streaming services were taken offline by a sudden surge in traffic. The attack continued for the duration of the event and then subsided. What was the most probable motivation behind this attack?

- (A) Espionage to intercept sensitive communications
- (B) **To cause a service disruption during the sports event**
- (C) Data exfiltration for future ransom demands
- (D) To gain unauthorized access and implant malware

Explanation 88. Correct Answer: B. To cause a service disruption during the sports event. The surge in traffic specifically timed with the sports event and its subsequent subsiding after the event indicates a targeted intention to disrupt the service during the sports event.

Option A is incorrect. There is no indication in the scenario that the attacker was interested in intercepting communications, especially since the target was a broadcasting company and not a diplomatic or governmental agency.

Option C is incorrect. The scenario does not mention any exfiltration of data or follow-up ransom demands. The focus of the attacker was on disrupting the streaming service.

Option D is incorrect. Although taking services offline can sometimes be a cover for more malicious activities, there's no evidence in this scenario to suggest that malware was implanted or unauthorized access was achieved.

Question 89. A software development company has decided to host their applications in a multi-cloud environment. Before deploying, they are looking to enhance the security of their cloud-based resources. Which of the following is the BEST practice for hardening their cloud infrastructure?

- (A) Ensure that all cloud storage buckets or containers are publicly accessible for easier data sharing
- (B) Apply consistent security configurations and policies across all cloud providers**
- (C) Use the same SSH key pairs across all cloud instances for uniformity
- (D) Limit the use of Identity and Access Management (IAM) roles to senior staff only

Explanation 89. Correct Answer: B. Apply consistent security configurations and policies across all cloud providers. Maintaining consistent security configurations and policies across all cloud providers ensures that there are no weak links in the multi-cloud setup and reduces the complexity of managing multiple sets of policies.

Option A is incorrect. Making all cloud storage buckets or containers publicly accessible can expose sensitive data and is a common misconfiguration that leads to data breaches.

Option C is incorrect. Using the same SSH key pairs across all instances can be risky. If an attacker obtains the SSH key, they can gain unauthorized access to all instances that use that key.

Option D is incorrect. While it's important to limit access based on the principle of least privilege, IAM roles should be appropriately assigned to staff based on their responsibilities and not just their seniority. This ensures that users have the necessary permissions to do their jobs without unnecessary access to sensitive resources.

Question 90. RedFlare Solutions, a financial firm, is storing sensitive client data in a database. The Chief Information Security Officer (CISO) insists that the data should be unreadable even if it's intercepted during transmission or if the storage is compromised. Which encryption standard would best serve this requirement?

- (A) Symmetric encryption using a shared key
- (B) Hashing the data with a one-way function
- (C) **Encrypting the entire database using transparent data encryption**
- (D) Storing the data in a proprietary format

Explanation 90. Correct Answer: C. Encrypting the entire database using transparent data encryption. Transparent data encryption (TDE) encrypts the entire database, ensuring that data remains encrypted both at rest and during transmission. It

renders the data unreadable without the appropriate encryption keys.

Option A is incorrect. Symmetric encryption can make data unreadable, but it may pose challenges in key management and distribution, especially if the key is compromised.

Option B is incorrect. Hashing data makes it unreadable, but it's a one-way function. Once data is hashed, it cannot be retrieved or decrypted, making it unsuitable for encrypting stored data that needs to be accessed and read.

Option D is incorrect. Simply storing data in a proprietary format doesn't mean it's encrypted or unreadable. If someone understands or reverse engineers the format, the data can be read.

Question 91. XYZ Corporation is planning to deploy a new wireless infrastructure in their newly acquired office building. The IT manager wants to ensure optimal wireless coverage throughout the premises. Which of the following should the IT team prioritize before installing the wireless access points?

- (A) Purchase the most expensive wireless access points to ensure maximum range
- (B) **Conduct a site survey to determine the best locations for access points**
- (C) Deploy all access points near windows to enhance signal strength
- (D) Ensure all users have 5GHz capable devices

Explanation 91. Correct Answer: B. Conduct a site survey to determine the best locations for access points. A site survey will help identify the optimal placements for access points to achieve consistent and robust wireless coverage across the entire premises.

Option A is incorrect. While quality equipment is essential, the costliest access points might not always guarantee the best results. Placement and environment play crucial roles in wireless performance.

Option C is incorrect. Deploying access points near windows can cause signal leakage, potentially making the signal available outside the intended area and presenting a security risk.

Option D is incorrect. While ensuring users have 5GHz capable devices is a good practice, it doesn't relate directly to the optimal installation of wireless access points.

Question 92. A client disputes having signed a digital contract. The service provider needs to prove that the signature was indeed from the client and hasn't been tampered with. Which of the following security concepts is the service provider relying on?

- (A) Authentication
- (B) Confidentiality
- (C) **Non-repudiation**
- (D) Access Control

Explanation 92. Correct Answer: C. Non-repudiation. Non-repudiation ensures that a party in a dispute cannot deny the

authenticity of their actions. In this scenario, it would provide evidence that the client did sign the contract and that it hasn't been tampered with post-signature.

Option A is incorrect. Authentication confirms the identity of a user or system. While it plays a part in ensuring that the right person is accessing the system, it doesn't directly provide evidence about the actions post-authentication, like signing a contract.

Option B is incorrect. Confidentiality ensures that information is only accessible to those with the appropriate permissions. It doesn't provide evidence of an action being taken by a specific entity.

Option D is incorrect. Access Control determines who or what can view or use resources in a computing environment. It doesn't ensure the validity of actions taken within the system.

Question 93. A software company recently discovered a vulnerability in its popular application, which allowed unauthorized access to users' data. Before the company could release a patch, a group of hackers exploited the vulnerability but only to notify the users about it. They did not misuse any data. What is the most probable motivation behind this group's action?

- (A) Financial gain by selling the data
- (B) Political beliefs against the software company's operations
- (C) **Ethical concerns about user privacy and security**
- (D) Desire to disrupt the software company's services

Explanation 93. Correct Answer: C. Ethical concerns about user privacy and security. The hackers did not misuse the data but instead chose to inform the users about the vulnerability, suggesting their motivation was based on ethical considerations to ensure users are aware of potential threats to their privacy.

Option A is incorrect. The hackers did not sell or misuse the data, which means financial gain wasn't their primary objective.

Option B is incorrect. There's no indication that the hackers' actions were driven by political beliefs against the software company.

Option D is incorrect. While the hackers did exploit a vulnerability, they did not aim to disrupt the company's services but to inform users about the vulnerability.

Question 94. A healthcare institution suffered a breach where medical records of high-profile patients were extracted. The data was not sold or publicly disclosed. Instead, certain individuals were approached with their personal health information and were extorted for money. What is the primary motivation behind this cyber attack?

- (A) Political activism to expose vulnerabilities in healthcare
- (B) Personal animosity targeting the healthcare institution
- (C) **Financial gain through targeted extortion**
- (D) Spreading malware and expanding the botnet

Explanation 94. Correct Answer: C. Financial gain through targeted extortion. Approaching specific individuals with their

personal health data for the purpose of extortion indicates a clear motivation of financial gain.

Option A is incorrect. While political activists might expose vulnerabilities in sectors like healthcare, they generally do so to raise awareness rather than for personal financial gain.

Option B is incorrect. There's no evidence from the given scenario to suggest that the attack was fueled by personal animosity towards the institution.

Option D is incorrect. The attackers' actions did not revolve around spreading malware or increasing a botnet's size but rather focused on individual extortion based on exfiltrated data.

Question 95. A company wants to ensure that security incidents are detected and addressed as quickly as possible by on-duty personnel. Which of the following operational security controls would be BEST to implement for this purpose?

- (A) Deploying a Network Intrusion Prevention System (NIPS)
- (B) Establishing a 24/7 Security Operations Center (SOC)
- (C) Creating a company-wide security policy
- (D) Implementing end-to-end data encryption

Explanation 95. Correct Answer: B. Establishing a 24/7 Security Operations Center (SOC). A Security Operations Center (SOC) is an operational control that provides real-time monitoring, detection, and response to security incidents. With a

24/7 SOC, the company ensures that there is always personnel available to handle security incidents as they occur.

Option A is incorrect. Deploying a Network Intrusion Prevention System (NIPS) is a technical control. While it can prevent unauthorized activities on the network, it does not ensure that there is personnel available around the clock to address incidents.

Option C is incorrect. Creating a company-wide security policy is a managerial control. It sets the guidelines and procedures for security but does not ensure continuous monitoring and immediate response to incidents.

Option D is incorrect. Implementing end-to-end data encryption is a technical control that ensures data confidentiality. While it protects data, it does not ensure that incidents are detected and addressed by on-duty personnel in real-time.

Question 96. As part of improving their security posture, TechHive Inc. decided to review their existing password policies. The current policy requires employees to use at least one uppercase letter, one number, and one special character. However, they found that users mostly only make minimal changes to their passwords during resets. Which standard should be integrated into their policy to ensure passwords are more complex and unique over time?

- (A) Password history retention
- (B) Password expiration period

- (C) Account lockout duration
- (D) Maximum password age

Explanation 96. Correct Answer: A. Password history

retention. Password history retention ensures that users cannot reuse a certain number of previous passwords, forcing them to come up with unique passwords rather than making only minor changes to their current ones.

Option B is incorrect. The password expiration period dictates how long a password is valid before prompting the user for a change. While it can make users change passwords frequently, it doesn't prevent them from making minimal changes.

Option C is incorrect. Account lockout duration specifies the time an account remains locked after a predefined number of incorrect login attempts. It doesn't ensure password complexity or uniqueness over time.

Option D is incorrect. Maximum password age defines how long a password can be used before it must be changed. Like Option B, it doesn't prevent users from making minimal changes to their passwords.

Question 97. A medium-sized enterprise is concerned about the security of its office workstations after a series of malware infections. As a security analyst, which of the following recommendations would BEST improve the security baseline of the workstations?

- (A) Install multiple antivirus solutions to ensure maximum detection

- (B) Set up screensavers with cyber hygiene tips to educate users
- (C) **Disable unnecessary services and ports on the workstations**
- (D) Frequently change the desktop wallpaper to prevent monotony

Explanation 97. Correct Answer: C. Disable unnecessary services and ports on the workstations. By disabling unnecessary services and ports, you reduce the number of potential attack vectors and vulnerabilities, thus improving the security baseline of the workstations.

Option A is incorrect. Installing multiple antivirus solutions can lead to conflicts and may degrade system performance. It's better to have one robust, updated antivirus solution.

Option B is incorrect. While cyber hygiene tips can be informative, they don't directly contribute to the technical security baseline of a workstation.

Option D is incorrect. Changing the desktop wallpaper does nothing for security. Its primary purpose is aesthetics.

Question 98. After a significant merger between two large corporations, a comprehensive risk assessment was conducted to identify potential security gaps within the combined infrastructure. This assessment was exclusive to the merger and was not planned to be repeated in the future. What type of risk assessment was this?

- (A) Recurring

- (B) Continuous
- (C) **One-time**
- (D) Dynamic

Explanation 98. Correct Answer: C. One-time. A one-time risk assessment is a unique assessment carried out for a specific purpose or event, such as a merger, and is not repeated regularly like other types of assessments.

Option A is incorrect. Recurring risk assessments are conducted at regular intervals, such as annually or biannually.

Option B is incorrect. Continuous risk assessments involve ongoing monitoring of risks and do not refer to a single, specific assessment.

Option D is incorrect. Dynamic assessments continuously adapt to changing environments or factors, but this term does not denote a single, specific assessment.

Question 99. XYZ Corporation recently faced a major power outage that affected their primary data center. During the incident, it was found that there was no clear guidance on the steps to maintain or quickly restore business operations. To address this, which of the following policies should XYZ Corporation prioritize implementing?

- (A) Data Classification Policy
- (B) **Business Continuity Policy**
- (C) Acceptable Use Policy
- (D) Network Segmentation Strategy

Explanation 99. Correct Answer: B. Business Continuity

Policy. A Business Continuity Policy outlines the processes and procedures an organization should follow to ensure that essential functions can continue during and after a disaster. It provides a roadmap for maintaining and quickly restoring business operations.

Option A is incorrect. The Data Classification Policy is concerned with categorizing data based on its sensitivity but doesn't address continuity of business operations during disruptions.

Option C is incorrect. The Acceptable Use Policy specifies how the organization's IT resources and networks can be used by employees. It doesn't provide guidance on restoring business operations during a disaster.

Option D is incorrect. While Network Segmentation Strategy is crucial for security, dividing the network into segments does not specifically address business continuity during major disruptions.

Question 100. CyberFleet Inc., a software development company, has just heard of a newly discovered vulnerability in a third-party library they heavily rely upon. The security team quickly gathers to understand and analyze the potential risks associated with this vulnerability. This spontaneous assessment is best described as:

- (A) Routine
- (B) Ad hoc

- (C) Scheduled
- (D) Benchmark

Explanation 100. Correct Answer: B. Ad hoc. An ad hoc risk assessment is done in response to a specific event or situation and is not planned in advance.

Option A is incorrect. Routine assessments, similar to periodic ones, are performed at regular intervals and are not typically in response to sudden events.

Option C is incorrect. Scheduled risk assessments are planned and occur at predetermined times or intervals.

Option D is incorrect. Benchmark assessments are evaluations that compare an organization's processes or performance against a set standard or best practices in the industry.

EXAM SIMULATOR #2

Questions 101-200

Question 101. XYZ Corp is implementing a new vulnerability scanning solution. The security team wants a solution that does not require any software to be installed on the target machines but can still identify vulnerabilities. Which type of vulnerability scanning solution should they choose?

- (A) Host-based Intrusion Detection System (HIDS)
- (B) Agentless Vulnerability Scanner
- (C) Client-based Vulnerability Scanner
- (D) Host-based Intrusion Prevention System (HIPS)

Question 102. FinCorp, a financial institution, has recently adopted a new security framework. In this framework, every device and user inside the organization's network is treated as if they were outside the perimeter, necessitating rigorous verification processes even for internal requests. Which security paradigm has FinCorp implemented?

- (A) Demilitarized Zone (DMZ)
- (B) Network Segmentation
- (C) Intrusion Detection System (IDS)
- (D) Zero Trust

Question 103. An art gallery wants to deploy a security solution to detect movement in an open courtyard that features several sculptures. This space has varying temperature conditions,

which might cause false alarms in some motion detection technologies. Which type of sensor would be MOST appropriate to ensure consistent motion detection in such conditions?

- (A) Thermal imaging sensors
- (B) Pressure-sensitive mats
- (C) Ultrasonic detectors
- (D) Microwave motion detectors

Question 104. SecureNet, a cybersecurity firm, is implementing an Intrusion Detection System (IDS) for its enterprise client. Where should the IDS be placed for optimal detection of malicious activities?

- (A) Before the perimeter firewall to capture all inbound traffic
- (B) Between the perimeter firewall and the internal network to monitor the filtered traffic
- (C) Inside the DMZ to monitor only external service requests
- (D) Adjacent to each workstation for personalized security

Question 105. AcmeBank recently performed a business impact analysis for its online banking system. The result indicated that the bank could tolerate a maximum downtime of 4 hours for the system before incurring significant financial losses and customer dissatisfaction. Which concept best describes this 4-hour period?

- (A) Recovery Point Objective (RPO)
- (B) Maximum Tolerable Downtime (MTD)

- (C) Recovery Time Objective (RTO)
- (D) Time To Restore (TTR)

Question 106. A financial company wants to improve its web browsing security by intercepting and inspecting web traffic to prevent users from accessing malicious sites or downloading malware. They are looking for a solution that can act as an intermediary for requests from clients seeking resources from other servers. What should the company implement?

- (A) Network IDS
- (B) VPN Concentrator
- (C) Proxy server
- (D) Jump server

Question 107. A user receives an SMS claiming to be from her bank, alerting her of unauthorized activity on her account. The message instructs the user to immediately click on a provided link and verify her account details. The user hasn't noticed any irregularities with her bank account. Which type of attack is this SMS most likely part of?

- (A) Smishing
- (B) Vishing
- (C) Bluejacking
- (D) Bluesnarfing

Question 108. Jane, a security analyst, receives a report about network slowdowns happening at specific times of the day. After investigating, she discovers that a device is flooding the network with traffic, causing legitimate requests to be dropped. Which type of attack is this device likely performing?

- (A) Distributed Denial of Service (DDoS)

- (B) ARP poisoning
- (C) MAC flooding
- (D) DNS amplification

Question 109. During a major international sporting event, a group of unidentified hackers simultaneously launched cyberattacks against multiple infrastructures in the host city, including transportation networks, power grids, and telecommunication systems. There was no ransom demand or any clear financial motive behind the attacks. What is the most probable motivation behind these actions?

- (A) Financial gain from selling stolen data
- (B) Ethical concerns about the environmental impact of the sporting event
- (C) Revenge against a particular athlete or team
- (D) Desire to create disruption and chaos during the event

Question 110. A local coffee shop offers free Wi-Fi to its customers. Recently, there have been reports of man-in-the-middle attacks on the network. The owner decides to upgrade the wireless security and wants to implement a cryptographic protocol to secure data transmissions. Which protocol would provide a balance between security and performance for the public Wi-Fi users?

- (A) Advanced Encryption Standard (AES)
- (B) Wired Equivalent Privacy (WEP)
- (C) RC4 Stream Cipher
- (D) Open Wireless

Question 111. TechHive Corp. is planning to sell some of its old servers. Before selling, they want to ensure that no

retrievable personal or business data remains on the hard drives. Which of the following methods should TechHive use to ensure the drives are clean and the data cannot be recovered?

- (A) Simple Format
- (B) Magnetic Wiping
- (C) Physical Destruction
- (D) Standard Defragmentation

Question 112. A financial institution has reported that they experience an average of 3 phishing attacks every year that attempt to compromise their user data. Based on this data, what is the Annualized Rate of Occurrence (ARO) for these phishing attacks?

- (A) 0.33
- (B) 1
- (C) 3
- (D) 12

Question 113. TechFlow Corp. is undergoing a risk analysis for its online platform. If a critical vulnerability were exploited, the company would have to pay \$10,000 in repair costs, \$5,000 in compensation to customers, and a \$15,000 fine to regulatory bodies. What would be the Single Loss Expectancy (SLE) for this vulnerability?

- (A) \$10,000
- (B) \$20,000
- (C) \$30,000
- (D) \$50,000

Question 114. Country A and Country B are engaged in an ongoing territorial dispute. Suddenly, critical infrastructure

facilities in Country B, such as power plants and transportation hubs, experience systematic cyberattacks. No ransom demand is made, and the attacks lead to significant disruption. What is the most probable motivation behind these cyberattacks?

- (A) Financial gain from market disruptions
- (B) Ethical hackers testing vulnerabilities
- (C) Disruption due to philosophical disagreements with Country B's policies
- (D) Acts of cyberwarfare to weaken Country B's position

Question 115. The IT security team at a large corporation is evaluating monitoring tools for network traffic. They need a solution that can inspect network packets without introducing any potential latency or altering the network flow. Which type of device attribute should they consider?

- (A) Active IDS
- (B) Passive firewall
- (C) Active firewall
- (D) Passive IDS

Question 116. In a routine security assessment, Claire found that a newly deployed database server within her organization is still using its default login credentials. Which of the following is the PRIMARY security risk associated with this finding?

- (A) The database will not function optimally
- (B) The server will need frequent patches
- (C) Unauthorized individuals may easily gain access
- (D) The server will consume more bandwidth

Question 117. Mike, a network administrator, notices an unauthorized device connected directly to the company's main

network switch in the server room. This device is attempting to capture network traffic. What kind of attack is this unauthorized device likely conducting?

- (A) Rogue access point
- (B) VLAN hopping
- (C) Port mirroring
- (D) ARP poisoning

Question 118. GreenValley Mall, located in a busy urban area, has recently faced security concerns due to the proximity of its main entrance to a major road. Which physical security enhancement can the mall management implement to create a protective barrier between the road and the entrance, ensuring pedestrian safety and preventing unauthorized vehicular access?

- (A) Reinforced Walls
- (B) Metal Detectors
- (C) Bollards
- (D) Perimeter Fencing

Question 119. TechCorp is implementing a new cloud-based solution. The security team has been tasked with analyzing the risks associated with this project. They've decided to categorize the risks based on their potential impact levels: Low, Medium, High, and Critical. Which type of risk analysis is TechCorp's security team employing?

- (A) Quantitative
- (B) Statistical
- (C) Qualitative
- (D) Financial

Question 120. TechBlitz Inc. recently underwent an IT audit, and one of the suggestions was to reduce the attack surface. Which of the following measures would be MOST effective in accomplishing this?

- (A) Increasing the password length requirement for all users
- (B) Implementing regular vulnerability assessments
- (C) Deactivating unused services and ports on servers
- (D) Implementing a strict BYOD (Bring Your Own Device) policy

Question 121. GreenTech, a data center company, is planning to expand its operations in a region known for frequent power outages. To maintain security posture and ensure continuity of operations, which of the following should be their PRIMARY consideration regarding power?

- (A) Using power-efficient servers to reduce electricity costs
- (B) Setting up solar panels to promote green energy
- (C) Investing in redundant power supplies and uninterruptible power systems (UPS)
- (D) Running operations only during peak daylight hours to ensure natural lighting

Question 122. WebFlix, a popular online movie streaming service, experienced a data center outage due to a natural disaster. They had backups in place and restored their systems using data from 6 hours prior to the outage. This resulted in the loss of some user interactions, like ratings and watchlists from the last 6 hours. What term describes the 6-hour gap between the last backup and the time of the outage?

- (A) Recovery Time Objective (RTO)
- (B) Maximum Tolerable Downtime (MTD)
- (C) Recovery Duration Period (RDP)
- (D) Recovery Point Objective (RPO)

Question 123. Jane, the CISO at a financial institution, is overseeing the decommissioning of several old servers. She is aware that while some data must be destroyed, other data must be retained due to industry regulations. Which principle should Jane primarily focus on to ensure compliance?

- (A) Minimum necessary principle
- (B) Principle of least privilege
- (C) Data retention policy
- (D) Mandatory vacation policy

Question 124. A medium-sized e-commerce company recently experienced a data breach due to an external attack. Post-incident analysis revealed that while there were indications of the attack in their network traffic, no alarms were raised at the time of the attack. The company now wants to implement a solution to actively monitor and take action against malicious network traffic. Which of the following should they deploy?

- (A) Intrusion Detection System (IDS)
- (B) Network Access Control (NAC)
- (C) Proxy server
- (D) Intrusion Prevention System (IPS)

Question 125. A cybersecurity analyst at XYZ Corp is looking to deploy a system that appears to be vulnerable and enticing to attackers. The main goal is to study the tactics, techniques, and procedures (TTPs) of potential adversaries, without them

realizing that they're interacting with a decoy. Which of the following would BEST meet this requirement?

- (A) Intrusion Detection System (IDS)
- (B) Firewall
- (C) Honeypot
- (D) VPN Concentrator

Question 126. The networking team at SecureNet Corp. is setting up a new branch office. They want to ensure secure connectivity between the branch office and the main office. Which of the following would BEST provide this?

- (A) Establishing a clear line of sight for wireless antennas between the two locations
- (B) Implementing a Virtual Private Network (VPN) between the two sites
- (C) Increasing bandwidth on the public internet connection at both locations
- (D) Using multi-factor authentication for all user accounts in both locations

Question 127. TechVault, a company specializing in secure storage solutions, recently had an unauthorized intrusion where a burglar managed to bypass their motion sensors. In a bid to prevent future breaches, they are considering deploying a system that can detect weight changes in a restricted floor area to alert any unauthorized access. Which of the following would be BEST for this requirement?

- (A) Ultrasonic motion detectors
- (B) Pressure-sensitive floor mats
- (C) CCTV cameras with facial recognition
- (D) Glass break sensors

Question 128. SafeMed, a medical facility, uses a life-saving medical device with embedded software. Recently, a security vulnerability was found in the software, but due to the device's FDA regulatory status and the software's design, it cannot be patched immediately. How should SafeMed address the security concerns related to this device?

- (A) Disconnect the device from all networks and only use it in standalone mode
- (B) Inform patients about the vulnerability and let them decide whether to use the device
- (C) Implement network segmentation and strictly control access to the device
- (D) Return the device to the manufacturer for a full refund

Question 129. The network administrator at a university wants to ensure that when students log onto the campus wireless network, their credentials are verified by the university's central authentication server. Additionally, the administrator wants to make sure that the data between the wireless access point and the central server is encrypted. Which solution should the administrator implement?

- (A) WPA3 with SAE
- (B) WPA2-Personal with AES
- (C) WPA2-Enterprise with RADIUS
- (D) Open wireless with VPN

Question 130. TechHaus has recently experienced multiple security breaches where unauthorized personnel have managed to infiltrate their server rooms after hours. To enhance security measures, the company decided to deploy a new system. Which of the following options would BEST detect human intruders

based on their body heat even in complete darkness?

- (A) Installing CCTV cameras with LED lights
- (B) Using ultrasonic motion sensors
- (C) Deploying infrared (IR) sensors
- (D) Implementing RFID badge readers at the entrance

Question 131. SecureTech Corp, a company dealing with sensitive client data, is redesigning its main office entrance to enhance security. They want to ensure that only one person gains access at a time, even if multiple people try to enter using a single authorized access badge. Which of the following would best serve this purpose?

- (A) CCTV Cameras
- (B) Mantrap
- (C) Biometric Scanners
- (D) Motion Detectors

Question 132. An enterprise wants to configure its firewall so that if a malfunction occurs, the firewall should automatically allow traffic to ensure business continuity. Which failure mode should be implemented?

- (A) Fail-safe
- (B) Fail-over
- (C) Fail-closed
- (D) Fail-open

Question 133. During a board meeting at DataFlow Corp., the CEO emphasizes that while they are willing to take certain risks for innovation, there's a limit to the amount of risk they are willing to take, especially concerning potential financial losses. To ensure that risks stay below this level, what should be

defined in the risk register?

- (A) Risk Owner Assignment
- (B) Key Risk Indicator (KRI)
- (C) Risk Impact Analysis
- (D) Risk Threshold

Question 134. A healthcare provider is updating its network infrastructure. Due to the sensitive nature of the medical data they handle, they want to ensure that any anomalies or malicious activities in the network are immediately detected and alerted. Which system should they primarily consider?

- (A) Intrusion Prevention System (IPS)
- (B) Intrusion Detection System (IDS)
- (C) DHCP server
- (D) VPN concentrator

Question 135. BioGen Inc., a biotechnology company, has implemented a layered security approach. They are considering adding a human element to their security measures for their research labs. Which of the following would best provide the ability to evaluate and respond to various security situations with human judgment?

- (A) Installing biometric locks
- (B) Employing security guards
- (C) Implementing an access control vestibule
- (D) Deploying AI-driven security cameras

Question 136. ExamsDigest Corp, a technology company, recently conducted a security assessment to align with industry best practices. The company's current security posture was compared to its desired future state, revealing discrepancies.

Which of the following best describes the approach ExamsDigest Corp employed?

- (A) Vulnerability Assessment
- (B) Penetration Testing
- (C) Gap Analysis
- (D) Threat Modeling

Question 137. Sophia, the CFO of a medium-sized company, received a call from an individual claiming to be from the IT department. The caller requested her login details for a “critical system update.” Suspecting something wasn’t right, Sophia hung up and contacted her IT department, which confirmed no such call was made by them. Which type of attack did Sophia most likely experience?

- (A) Vishing
- (B) Phishing
- (C) SQL Injection
- (D) Cross-Site Request Forgery (CSRF)

Question 138. A medium-sized enterprise is preparing to upgrade its office workstations. The IT department is considering purchasing devices from a lesser-known, but cheaper, vendor. Which of the following should be the PRIMARY consideration before finalizing the acquisition?

- (A) Whether the vendor offers a longer warranty period
- (B) The aesthetics and design of the workstations
- (C) The vendor's adherence to industry security standards and practices
- (D) The amount of training required for IT staff to support the new devices

Question 139. An employee of XYZ Corp downloaded a seemingly benign PDF file from a vendor's website. After opening the PDF, the company's intrusion detection system (IDS) alerted the security team about suspicious activity originating from the employee's computer. The PDF file most likely contained which of the following threats?

- (A) Watering Hole Attack
- (B) Malicious Macro
- (C) SQL Injection
- (D) Credential Harvesting

Question 140. A rapidly growing e-commerce platform has been facing intermittent downtimes, especially during sale events. To ensure high availability and even distribution of traffic among servers, the company is considering deploying a specific type of network appliance. Which of the following should the company deploy?

- (A) Intrusion Detection System (IDS)
- (B) VPN concentrator
- (C) Load balancer
- (D) Proxy server

Question 141. TechFusion Inc. is a well-established technology company that has been in the market for over 15 years. Recently, the board of directors decided that the company will pursue aggressive growth strategies by entering new, untested markets and launching cutting-edge products, even if these strategies come with significant risks. How would you classify TechFusion Inc.'s risk appetite?

- (A) Conservative
- (B) Expansionary

- (C) Neutral
- (D) Risk-averse

Question 142. Alex, an employee at XYZ Corp, noticed an unfamiliar USB drive lying in the company parking lot. Out of curiosity, Alex plugged the device into his workstation. Almost immediately, his antivirus program detected malicious software trying to execute. What type of attack did Alex likely encounter?

- (A) Man-in-the-Middle Attack
- (B) Evil Twin
- (C) Spear Phishing
- (D) USB Drop Attack

Question 143. A rapidly growing e-commerce company has recently experienced an increase in cross-site scripting (XSS) and SQL injection attacks. The company wants to deploy a solution that specifically protects against these threats at the application layer. Which type of firewall would be most appropriate?

- (A) Stateful Packet Inspection Firewall
- (B) Proxy Firewall
- (C) Network Layer Firewall
- (D) Web Application Firewall (WAF)

Question 144. A financial institution wants to enhance the security of its wired network. The goal is to ensure that only authorized devices can connect to the network, and the authentication process should be based on credentials or digital certificates. Which of the following protocols would best serve this purpose?

- (A) SNMPv3
- (B) SSL/TLS
- (C) 802.1X EAP
- (D) DHCP

Question 145. An organization is evaluating different security solutions for their new branch office. They want to ensure that the chosen solution can be rapidly deployed with minimal configuration. Which of the following options BEST fulfills this requirement?

- (A) A customized Intrusion Prevention System (IPS) tailored to the organization's unique needs
- (B) A zero-touch provisioning firewall
- (C) An open-source firewall with extensive manual settings
- (D) A security information and event management (SIEM) solution requiring manual log source integration

Question 146. A company named TechFlow is planning to produce a new line of smart home devices. They have opted to use a single supplier for a crucial component in their devices. Which of the following represents the MOST significant security risk associated with this decision?

- (A) It will be challenging to negotiate prices with just one supplier
- (B) If the supplier's delivery timeline is delayed, product launch might be postponed
- (C) A compromise at the supplier could lead to vulnerabilities in all devices
- (D) TechFlow will need to rely on the supplier's warranty and return policies

Question 147. The security team of a multinational company deployed a network of honeypots globally, making it appear as an interconnected and realistic environment. They aim to study coordinated multi-stage attacks. This deceptive setup is known as:

- (A) Firewall Cluster
- (B) Virtual LAN (VLAN)
- (C) Distributed Denial of Service (DDoS) Prevention
- (D) Honeynet

Question 148. David, an IT administrator, noticed an unusually high data usage on several company-owned mobile devices even when they are connected to the corporate Wi-Fi. He suspects these devices might be using cellular data in the background. Which of the following solutions should David implement to ensure that company devices use only the corporate Wi-Fi for data transactions when they're in the office?

- (A) Enable Airplane mode on all devices
- (B) Set up a Wi-Fi whitelist
- (C) Implement a mobile device management (MDM) policy to prioritize Wi-Fi
- (D) Disable cellular antennas in the office area

Question 149. A university is looking to revamp its wireless network to provide secure access for students and faculty. The IT department wants an authentication method that leverages a centralized server to validate user credentials and can integrate with their existing directory service. Which authentication protocol should they consider?

- (A) Pre-shared Key (PSK)
- (B) Lightweight Extensible Authentication Protocol

(LEAP)

(C) Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)

(D) Shared Secret Challenge

Question 150. A university is looking to revamp its wireless network to provide secure access for students and faculty. The IT department wants an authentication method that leverages a centralized server to validate user credentials and can integrate with their existing directory service. Which authentication protocol should they consider?

(A) Pre-shared Key (PSK)

(B) Lightweight Extensible Authentication Protocol

(LEAP)

(C) Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)

(D) Shared Secret Challenge

Question 151. CyberGuard LLC, a cybersecurity firm, is in a stable position in its industry with consistent returns. The leadership decides not to pursue aggressive growth strategies but instead chooses to maintain its current market share and operational scale. They are open to minor risks but avoid major disruptions. How can one best describe CyberGuard LLC's risk appetite?

(A) Expansionary

(B) Neutral

(C) Conservative

(D) Aggressive

Question 152. After a series of cyber-attacks on a company's infrastructure, the IT team decided to deploy a solution that would seem like a legitimate part of their network but is intentionally isolated and monitored. They intend to detect and analyze malicious activities in this isolated environment. What technology are they most likely implementing?

- (A) Network segmentation
- (B) Honeypot
- (C) DMZ (Demilitarized Zone)
- (D) Sandboxing

Question 153. Your organization is considering a partnership with TechVendor Inc., a software solution provider. Before finalizing the agreement, you wish to ensure their application's security. What would be the most direct method to assess the robustness of their system against potential cyber threats?

- (A) Conducting an internal security awareness training
- (B) Reviewing their past audit reports
- (C) Implementing strict firewall rules
- (D) Performing a penetration test on their application.

Question 154. An e-commerce platform recently suffered a data breach where attackers exploited cookies to impersonate user sessions. A security analyst is tasked with recommending measures to secure user cookies. Which of the following measures will ensure that cookies are transmitted securely between the user's browser and the server?

- (A) Storing cookies in the database
- (B) Implementing the "Secure" attribute for cookies
- (C) Increasing the cookie expiration time
- (D) Base64 encoding the cookie content

Question 155. An organization has recently received a new software patch for its critical infrastructure. Before deploying it to production, the security team wants to understand its behavior and ensure it doesn't contain any malicious code. Which of the following methods would be MOST effective for safely executing and observing the patch's behavior?

- (A) Deploying the patch during a maintenance window
- (B) Running the patch within a sandbox environment
- (C) Conducting a code review of the patch
- (D) Installing the patch on a virtual machine

Question 156. A recently hired security analyst at CyberTech Inc. wants to get a better understanding of the organization's network infrastructure. Which of the following activities would provide a LIST of servers, workstations, printers, switches, and routers currently active in the network?

- (A) Vulnerability Scanning
- (B) Intrusion Detection
- (C) Network Enumeration
- (D) Penetration Testing

Question 157. Tech Enterprises is planning to release a new product. As part of the product's creation, they've sourced components from various vendors. The security team is tasked with assessing risks linked to the supply chain. Which of the following is the MOST concerning risk when sourcing components from multiple vendors?

- (A) Difficulty in tracking product warranty details from multiple vendors
- (B) Increased product assembly time due to varied vendor delivery timelines

- (C) Potential for introduction of insecure or compromised components
- (D) The need for multiple purchase orders, leading to increased paperwork

Question 158. John, a security analyst, noticed an increase in unauthorized devices connecting to the company's wireless network. To identify the reason, he realized that the wireless access points were still using an old encryption standard. Which outdated encryption standard is likely in use that is known to be easily compromised?

- (A) WPA3
- (B) WEP
- (C) WPA2-PSK
- (D) AES

Question 159. After being fired from his position as a senior network administrator at XYZ Corp, John discovered a backdoor into the company's main server that he had previously set up. He then initiated a series of Distributed Denial of Service (DDoS) attacks over a month. What is the most probable motivation behind John's actions?

- (A) Ethical concerns about the company's data handling
- (B) Financial gain by selling access to the backdoor
- (C) Desire to research and find vulnerabilities for personal growth
- (D) Revenge against the company for his termination

Question 160. TechBank has just opened a new branch in the city center. Due to its location, the management is concerned about potential vehicular attacks on the facility. Which of the

following physical security measures can TechBank employ to specifically deter such attacks?

- (A) Surveillance Cameras
- (B) Bollards
- (C) Access Badges
- (D) Security Guards

Question 161. A financial organization's high-security data center has an authentication system for its main entry. If the system encounters an unexpected error, the organization wants to ensure that no one can gain access to the data center until the system is fixed. Which configuration should the authentication system be set to?

- (A) Fail-open
- (B) Fail-closed
- (C) Fail-secure
- (D) Fail-passive

Question 162. CyberSecure Inc. is evaluating the financial impact of a potential security breach on its main server. The company has estimated that a breach of this server would lead to a direct financial loss of \$500,000 due to data recovery, legal fees, and fines. Which of the following best represents this estimation?

- (A) Annual Rate of Occurrence (ARO)
- (B) Total Cost of Ownership (TCO)
- (C) Single Loss Expectancy (SLE)
- (D) Annualized Loss Expectancy (ALE)

Question 163. A large e-commerce company wants to ensure that their newly developed application is free from any code

vulnerabilities before it is deployed to the production environment. They want to catch any software flaws, especially those that might lead to potential security risks. Which of the following methodologies should they employ?

- (A) Runtime application self-protection (RASP)
- (B) Penetration testing on the live application
- (C) Static code analysis
- (D) User acceptance testing (UAT)

Question 164. In the new branch of BankSecure, the management has decided to install a security system at the main entrance that forces visitors to go through two separate authorization checks before entering the main premises. Which physical security measure should they consider?

- (A) Turnstiles
- (B) Security Guards
- (C) Access Control Vestibule
- (D) Keycard Readers

Question 165. XYZ Corporation recently implemented a security solution that constantly evaluates the company's threat landscape, monitoring for emerging risks and immediately alerting the security team of any changes. This assessment model allows the team to rapidly adapt their security posture in response to live threats. What type of risk assessment is XYZ Corporation utilizing?

- (A) One-time
- (B) Periodic
- (C) Dynamic
- (D) Continuous

Question 166. A software development company is evaluating the risks associated with a newly discovered vulnerability in its application. After reviewing logs and simulating potential attacks, the security team estimates that there is a 0.25 probability of the vulnerability being exploited in the next year. What does this probability indicate?

- (A) The vulnerability has a 1 in 4 chance of being exploited in the next year
- (B) The vulnerability will certainly be exploited four times in the next year
- (C) The vulnerability has been exploited 25 times in the past year
- (D) Every fourth customer will exploit the vulnerability.

Question 167. During a routine scan, the security team at a graphic design firm discovers that an employee downloaded an image from an email and subsequently, unusual network traffic was detected originating from that employee's workstation. The image appeared normal when opened. What type of attack might have been used in this situation?

- (A) Image Steganography Malware
- (B) Password Brute Force
- (C) Phishing
- (D) Port Scanning

Question 168. TechSoft Corp. is implementing a new asset-tracking system to monitor its vast array of computing resources. Which of the following should be the PRIMARY reason for maintaining an up-to-date hardware and software inventory?

- (A) To ensure software licenses are renewed on time

- (B) To identify and respond to unauthorized devices or software promptly
- (C) To aid in the procurement of new hardware and software
- (D) To provide employees with an understanding of available resources

Question 169. Acme Corp, a large organization, has recently entered into a contract with Zenith MSP for IT management and support. The CISO of Acme Corp is concerned about the security risks associated with this new relationship. Which of the following is the PRIMARY security concern when utilizing managed service providers (MSPs) in a supply chain?

- (A) Increased costs due to the integration of new technologies
- (B) Difficulty in ensuring consistent patch management
- (C) Potential for unauthorized access to company resources
- (D) Decreased IT staff morale due to outsourcing

Question 170. Mike, an employee at a tech company, receives an instant message from a coworker named Jessica. The message contains a link and claims to showcase a hilarious video. However, Mike knows Jessica is on vacation. He suspects the message might not genuinely be from her. What type of threat is Mike most likely encountering?

- (A) Watering Hole Attack
- (B) Man-in-the-Middle Attack
- (C) IM Spoofing
- (D) Side-channel Attack

Question 171. At a newly established museum, management wants to install sensors in the exhibit rooms to detect any unauthorized movement after hours. The rooms are often filled with a mix of air conditioning and external noise from the city. Which sensor would be BEST suited to detect movement in such conditions without being affected by the noise?

- (A) Acoustic sensors
- (B) Glass break detectors
- (C) Ultrasonic sensors
- (D) Thermal imaging cameras

Question 172. A global e-commerce company maintains a risk register to keep track of identified risks and to monitor specific metrics that might indicate an increased risk level. Recently, there has been a 20% increase in abandoned shopping carts on their platform. How should this metric be categorized in the context of the risk register?

- (A) Risk Appetite
- (B) Risk Mitigation Strategy
- (C) Key Risk Indicator (KRI)
- (D) Risk Tolerance Threshold

Question 173. An IT security analyst at a multinational corporation receives an email from the “HR Department” requesting urgent verification of his personal details, including his home address and social security number. The email has the company’s logo but has several spelling errors. Which type of email-based threat is this email most likely representing?

- (A) Business Email Compromise (BEC)
- (B) Email bombing

- (C) Email forwarding
- (D) Phishing

Question 174. TechSoft Corp, a mid-sized software development firm, is relocating its main office to a new building. The management is concerned about potential threats after hours, particularly due to the increasing reports of cyber-espionage. They are evaluating different security measures. Which option would provide an immediate physical presence and deterrence during non-business hours?

- (A) CCTV with motion detection
- (B) Retinal scan at all entrances
- (C) Security guard presence
- (D) Reinforced doors and windows

Question 175. A multinational corporation has data centers located in different countries. Due to regulatory constraints, remote access to these data centers is highly restricted. The company's IT administrators need a centralized way to access all data centers securely without directly accessing them from their workstations. Which solution should the company consider?

- (A) Setting up a DMZ
- (B) Implementing a Jump server
- (C) Deploying an Active Directory
- (D) Using a local Proxy

Question 176. GammaTech is in the final stages of deploying a new application. Before the deployment, the security team wants to examine the application's code without executing it to identify any potential vulnerabilities. Which vulnerability

identification method should the team employ?

- (A) Penetration Testing
- (B) Dynamic Analysis
- (C) Static Analysis
- (D) Fuzz Testing

Question 177. A cloud-based SaaS company wants to ensure its infrastructure can handle a potential influx of a large number of users in the future. Which of the following approaches would BEST meet this scalability consideration?

- (A) Implement a horizontal scaling strategy
- (B) Introduce multi-factor authentication
- (C) Deploy deep packet inspection tools
- (D) Implement a centralized logging system

Question 178. WebServ Corp., a web hosting company, has been analyzing the reliability of its servers. They found that one of their server models, on average, tends to fail once every 2000 hours and then gets promptly repaired. Which of the following metrics is WebServ Corp. evaluating?

- (A) Recovery Time Objective (RTO)
- (B) Mean Time To Repair (MTTR)
- (C) Mean Time Between Failures (MTBF)
- (D) Recovery Point Objective (RPO)

Question 179. Sarah, an end-user, downloads a software update from a website. Before installing, she wants to make sure the software hasn't been modified maliciously and that it originates from a trusted source. What should Sarah check to validate this?

- (A) The SSL certificate of the website
- (B) The application's code signing certificate

- (C) The application's open-source repositories
- (D) The software's user reviews

Question 180. An organization is conducting a risk assessment for its cloud infrastructure. The assessment has determined that the likelihood of a data breach through an insecure API is “High.” What factors may have contributed to this likelihood rating?

- (A) The API has been thoroughly tested and has a known secure configuration
- (B) There are few records of this kind of breach in the industry
- (C) The API is publicly accessible and has had several vulnerabilities reported in the past six months
- (D) The cloud provider offers a guaranteed SLA against any form of security breach

Question 181. Jenny, the new CIO of a multinational firm, wants to ensure that every software and hardware asset in the organization has a clearly defined owner responsible for its security and maintenance. Which of the following is the MOST effective way to achieve this?

- (A) Deploy an automated asset discovery tool and assign assets to departments based on their location
- (B) Mandate that every department head is the default owner of all assets within their department
- (C) Conduct regular audits and require individual users to claim ownership of their assets
- (D) Introduce an Asset Management System where assets are logged with defined ownership as they are procured or assigned

Question 182. An organization is deploying new IoT devices in its smart office. To ensure that only authorized devices can connect to the corporate network, each device will be given a unique key pair. Which of the following best describes the system authentication approach the organization is using?

- (A) Shared secret authentication
- (B) Public key infrastructure (PKI)
- (C) Token-based authentication
- (D) Username and password authentication

Question 183. After a recent security breach, CyberCorp is reviewing its software vendors for their responsiveness to vulnerabilities. Which of the following metrics would BEST assist CyberCorp in determining the timeliness and efficiency of security patches from a vendor?

- (A) The frequency of software updates released by the vendor
- (B) The vendor's quarterly financial reports
- (C) Time between vulnerability disclosure and patch release by the vendor
- (D) The number of features added by the vendor in the last software update

Question 184. A company is setting up a secure communication channel between its headquarters and a remote branch office. To ensure that data transmitted over this channel originates from a legitimate system at the branch office, the company is considering using digital certificates. Which authentication method for systems is the company contemplating?

- (A) Kerberos authentication
- (B) Password-based authentication

- (C) Certificate-based authentication
- (D) Biometric-based authentication

Question 185. After a series of cyber incidents, AlphaTech Corp. wants to take proactive measures to identify vulnerabilities in their network. They aim to obtain a comprehensive report of potential weaknesses without exploiting them. Which of the following would best meet this objective?

- (A) Penetration test
- (B) Vulnerability scan
- (C) Red team assessment
- (D) Port security

Question 186. Lucy, a security analyst, is informed that several employees have been receiving unauthorized file transfer requests via Bluetooth when they are in the company's cafeteria. Which of the following attacks is MOST likely being attempted?

- (A) Bluejacking
- (B) ARP poisoning
- (C) Bluesnarfing
- (D) Evil Twin

Question 187. A small business wants to deploy a single network security device that can handle multiple security functions such as firewall protection, intrusion detection, anti-malware, and content filtering. Which of the following would be the most suitable solution?

- (A) Network Intrusion Detection System (NIDS)
- (B) Web Application Firewall (WAF)

- (C) Unified Threat Management (UTM)
- (D) Proxy Server

Question 188. During an audit review at NetSecure Corp., the external auditors observed that the company is willing to take risks that can potentially result in a 10% decrease in their annual profits, but no more than that. The auditors want to document this finding in their report. Which term should they use to describe NetSecure Corp.'s stance?

- (A) Risk Avoidance
- (B) Risk Transfer
- (C) Risk Tolerance
- (D) Risk Assessment

Question 189. SecureWeb LLC, a web hosting company, has experienced two server breaches over the past five years. They are currently analyzing the risks associated with their infrastructure. Which of the following best represents the Annualized Rate of Occurrence (ARO) for the server breaches?

- (A) 0.2
- (B) 0.4
- (C) 2
- (D) 5

Question 190. DataCenter Inc. is located in a region prone to protests and vandalism. They wish to enhance their perimeter security to deter potential intruders and make it visibly clear that unauthorized access is restricted. Which of the following physical security measures would be the most effective first line of defense for the company?

- (A) Sliding Doors

- (B) Security Cameras
- (C) High-security Fencing
- (D) Proximity Card Readers

Question 191. A financial institution is shutting down one of its data centers. Given the highly sensitive nature of the data stored, the company wants to ensure that there is no possibility of data retrieval from the storage devices. Which of the following methods would be the MOST effective in guaranteeing the destruction of data?

- (A) Overwriting with zeros
- (B) Standard Disk Format
- (C) Physical Destruction
- (D) Running a Disk Cleanup utility

Question 192. Maria, a network administrator, receives a report detailing several open service ports on critical company servers. She wants to verify the accuracy of the report. Which of the following tools would be BEST for Maria to use to validate the findings?

- (A) Password cracker
- (B) Port scanner
- (C) IDS (Intrusion Detection System)
- (D) Web application firewall

Question 193. Acme Corp is restructuring its internal network to improve its security posture. They aim to separate areas with different levels of trust. Which of the following approaches would BEST achieve this objective?

- (A) Implementing VLANs based on organizational departments

- (B) Setting up a perimeter firewall to segment external and internal traffic
- (C) Designing network zones based on data sensitivity and access requirements
- (D) Using a single, flat network for simplicity

Question 194. A company has recently upgraded its wireless infrastructure and wants to ensure that the data transmitted over its wireless network is protected using the most recent and secure encryption standards. Which of the following should the company configure on its wireless access points?

- (A) WEP
- (B) WPA
- (C) WPA2
- (D) WPA3

Question 195. AlphaTech is conducting a risk analysis on their new online payment gateway. They've calculated the Annual Rate of Occurrence (ARO) for a specific vulnerability as 2, and the Single Loss Expectancy (SLE) as \$50,000. How much should AlphaTech anticipate losing annually due to this vulnerability?

- (A) \$10,000
- (B) \$100,000
- (C) \$25,000
- (D) \$1,000,000

Question 196. After a recent security breach, CyberSolutions Inc. evaluated their response metrics and determined that, on average, it took 4 hours from identifying a security breach to having it completely resolved. Which metric best describes this

4-hour timeframe?

- (A) Recovery Time Objective (RTO)
- (B) Recovery Point Objective (RPO)
- (C) Mean Time Between Failures (MTBF)
- (D) Mean Time To Repair (MTTR)

Question 197. A financial application allows users to transfer money to other accounts by entering the account number and the amount to transfer. During a security audit, it was observed that malicious users could enter SQL code into the account number field to manipulate the application's database. Which security technique should the development team implement to address this vulnerability?

- (A) Code obfuscation
- (B) Input validation
- (C) Encryption at rest
- (D) Session timeout

Question 198. GreenTech Inc. is selling a set of old servers to another company. Before the transaction, they want to ensure the data on these servers is irretrievable and they can prove that due diligence was performed. What should GreenTech seek to assure the buyer of proper data destruction?

- (A) A receipt of sale for the servers
- (B) A detailed log of the server's usage
- (C) A certificate of data sanitization
- (D) A user manual of the servers

Question 199. A healthcare organization uses a software platform to manage patient records. A recent vulnerability assessment identified a potential exploit where an unauthorized

individual might gain access to 30% of stored patient data.

Which of the following BEST describes this scenario?

- (A) The threat likelihood is 30%
- (B) The vulnerability has a 30% rate of occurrence
- (C) The exposure factor of the vulnerability is 30%
- (D) 30% of the patients have been impacted

Question 200. GreenTech Industries has a manufacturing facility located in a relatively secluded area. Recent incidents of theft and trespassing have alarmed the management. Which of the following would MOST effectively deter unauthorized nighttime access to the perimeter of the facility?

- (A) Installing infrared sensors
- (B) Using bright perimeter lighting
- (C) Deploying additional security guards inside the facility
- (D) Increasing the height of the facility walls

Answers 101-200

Question 101. XYZ Corp is implementing a new vulnerability scanning solution. The security team wants a solution that does not require any software to be installed on the target machines but can still identify vulnerabilities. Which type of vulnerability scanning solution should they choose?

- (A) Host-based Intrusion Detection System (HIDS)
- (B) **Agentless Vulnerability Scanner**

- (C) Client-based Vulnerability Scanner
- (D) Host-based Intrusion Prevention System (HIPS)

Explanation 101. Correct Answer: B. Agentless

Vulnerability Scanner. An agentless vulnerability scanner does not require any software (agent) to be installed on the target systems. Instead, it remotely scans the systems and identifies vulnerabilities by checking against a database of known vulnerabilities.

Option A is incorrect. Host-based Intrusion Detection System (HIDS) monitors the internal workings of a computing system, not for vulnerabilities but for signs of unauthorized or malicious activity.

Option C is incorrect. Client-based Vulnerability Scanner requires an agent or software component to be installed on the target system to perform the vulnerability assessment.

Option D is incorrect. Host-based Intrusion Prevention System (HIPS) is designed to detect and prevent malicious activity on a particular device, not to scan for vulnerabilities.

Question 102. FinCorp, a financial institution, has recently adopted a new security framework. In this framework, every device and user inside the organization's network is treated as if they were outside the perimeter, necessitating rigorous verification processes even for internal requests. Which security paradigm has FinCorp implemented?

- (A) Demilitarized Zone (DMZ)
- (B) Network Segmentation

- (C) Intrusion Detection System (IDS)
- (D) **Zero Trust**

Explanation 102. Correct Answer: D. Zero Trust. Zero Trust is a security model that treats every access request with skepticism, regardless of its origin, be it from within or outside the organization's traditional perimeter. It requires rigorous verification processes for every interaction.

Option A is incorrect. A Demilitarized Zone (DMZ) is a physical or logical subnetwork that exposes an organization's external-facing services to a larger, untrusted network, usually the internet.

Option B is incorrect. Network Segmentation divides a network into multiple segments or subnets, allowing administrators to control the flow of traffic between them. It does not inherently distrust all traffic like Zero Trust.

Option C is incorrect. Intrusion Detection System (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. It doesn't define how trust is managed across interactions.

Question 103. An art gallery wants to deploy a security solution to detect movement in an open courtyard that features several sculptures. This space has varying temperature conditions, which might cause false alarms in some motion detection technologies. Which type of sensor would be MOST appropriate to ensure consistent motion detection in such conditions?

- (A) Thermal imaging sensors
- (B) Pressure-sensitive mats
- (C) Ultrasonic detectors
- (D) **Microwave motion detectors**

Explanation 103. Correct Answer: D. Microwave motion detectors. Microwave motion detectors are suitable for open areas and are less affected by temperature changes. They emit microwave beams to create an invisible detection zone and can consistently detect motion when an object interrupts this zone, irrespective of the ambient temperature.

Option A is incorrect. Thermal imaging sensors detect variations in heat. While they can be effective, the varying temperature conditions in the courtyard may cause inconsistencies in detection.

Option B is incorrect. Pressure-sensitive mats are designed to detect weight or pressure changes when stepped on. They would not be suitable for an open courtyard where movement needs to be detected across a larger area.

Option C is incorrect. Ultrasonic detectors emit sound waves to detect motion. However, they might also be affected by external environmental factors and are not as suitable for open courtyards as microwave motion detectors.

Question 104. SecureNet, a cybersecurity firm, is implementing an Intrusion Detection System (IDS) for its enterprise client. Where should the IDS be placed for optimal detection of malicious activities?

- (A) Before the perimeter firewall to capture all inbound traffic
- (B) **Between the perimeter firewall and the internal network to monitor the filtered traffic**
- (C) Inside the DMZ to monitor only external service requests
- (D) Adjacent to each workstation for personalized security

Explanation 104. Correct Answer: B. Between the perimeter firewall and the internal network to monitor the filtered traffic. By placing the IDS between the firewall and the internal network, it can monitor traffic that has passed through the firewall's filters. This position provides a balance between capturing potential threats and reducing false positives from benign external traffic.

Option A is incorrect. While placing the IDS before the firewall will capture all inbound traffic, it may result in a high number of false positives since a lot of benign traffic might trigger alarms.

Option C is incorrect. Placing the IDS only in the DMZ would limit its visibility to only external service requests and not the overall internal traffic which might have potential threats.

Option D is incorrect. While personal IDS on each workstation provides granular monitoring, it does not provide a holistic view of network activities and can be resource-intensive.

Question 105. AcmeBank recently performed a business impact analysis for its online banking system. The result indicated that the bank could tolerate a maximum downtime of 4 hours for the system before incurring significant financial losses and customer dissatisfaction. Which concept best describes this 4-hour period?

- (A) Recovery Point Objective (RPO)
- (B) Maximum Tolerable Downtime (MTD)
- (C) **Recovery Time Objective (RTO)**
- (D) Time To Restore (TTR)

Explanation 105. Correct Answer: C. Recovery Time Objective (RTO). The Recovery Time Objective (RTO) is the targeted duration of time within which a business process must be restored after a disruption in order to avoid unacceptable consequences. In this scenario, AcmeBank's RTO for its online banking system is 4 hours.

Option A is incorrect. Recovery Point Objective (RPO) describes the maximum age of files that an organization must recover from backup storage for normal operations to resume after a disaster. It doesn't refer to the time duration.

Option B is incorrect. Maximum Tolerable Downtime (MTD) is the longest period of time that a business process can be down before causing irreparable harm to the business. While related, the question specifically describes the RTO.

Option D is incorrect. Time To Restore (TTR) is often a metric to measure the time it takes to restore a particular process or system. However, the scenario directly describes an RTO.

Question 106. A financial company wants to improve its web browsing security by intercepting and inspecting web traffic to prevent users from accessing malicious sites or downloading malware. They are looking for a solution that can act as an intermediary for requests from clients seeking resources from other servers. What should the company implement?

- (A) Network IDS
- (B) VPN Concentrator
- (C) **Proxy server**
- (D) Jump server

Explanation 106. Correct Answer: C. Proxy server. A Proxy server serves as an intermediary between the user's computer and the internet. It intercepts web requests and can provide functions such as filtering web content, caching web requests, and inspecting traffic for security reasons.

Option A is incorrect. A Network Intrusion Detection System (IDS) monitors and detects malicious activities on a network but does not function as an intermediary for web requests.

Option B is incorrect. A VPN Concentrator provides secure remote access to an organization's network but doesn't act as an intermediary for web browsing requests.

Option D is incorrect. A Jump server is used for secure and auditable access to internal servers but isn't designed for intercepting web traffic.

Question 107. A user receives an SMS claiming to be from her bank, alerting her of unauthorized activity on her account. The

message instructs the user to immediately click on a provided link and verify her account details. The user hasn't noticed any irregularities with her bank account. Which type of attack is this SMS most likely part of?

- (A) Smishing
- (B) Vishing
- (C) Bluejacking
- (D) Bluesnarfing

Explanation 107. Correct Answer: A. Smishing. Smishing is a type of phishing attack where malicious actors use SMS to deceive individuals into providing sensitive information, typically by impersonating trusted organizations or contacts.

Option B is incorrect. Vishing refers to voice phishing, where attackers use voice calls instead of text or email to impersonate legitimate entities and scam victims.

Option C is incorrect. Bluejacking involves sending unsolicited messages to Bluetooth-enabled devices. It doesn't typically involve impersonating a legitimate entity for deceptive purposes.

Option D is incorrect. Bluesnarfing is a type of unauthorized access to or theft of information from a Bluetooth device. It doesn't involve deceptive SMS messages.

Question 108. Jane, a security analyst, receives a report about network slowdowns happening at specific times of the day. After investigating, she discovers that a device is flooding the network with traffic, causing legitimate requests to be dropped.

Which type of attack is this device likely performing?

- (A) Distributed Denial of Service (DDoS)
- (B) ARP poisoning
- (C) **MAC flooding**
- (D) DNS amplification

Explanation 108. Correct Answer: C. MAC flooding. MAC flooding is an attack that aims to flood the switch's MAC table with fake MAC addresses until the table overflows. Once it overflows, the switch acts as a hub broadcasting packets to all machines in the network. This can cause significant slowdowns and disruptions.

Option A is incorrect. A Distributed Denial of Service (DDoS) attack uses multiple compromised devices to flood a target with traffic, usually to overwhelm it and take it offline. The scenario describes an internal network slowdown, not an external attack on services.

Option B is incorrect. ARP poisoning is an attack where false ARP messages are sent over a local area network. It's used to link an attacker's MAC address with the IP address of another host. While it can cause disruptions, the primary intent is not to flood the network.

Option D is incorrect. DNS amplification is a type of DDoS attack where an attacker uses publically-accessible DNS servers to flood a target system with DNS response traffic. This does not fit the internal network flooding described in the scenario.

Question 109. During a major international sporting event, a group of unidentified hackers simultaneously launched cyberattacks against multiple infrastructures in the host city, including transportation networks, power grids, and telecommunication systems. There was no ransom demand or any clear financial motive behind the attacks. What is the most probable motivation behind these actions?

- (A) Financial gain from selling stolen data
- (B) Ethical concerns about the environmental impact of the sporting event
- (C) Revenge against a particular athlete or team
- (D) **Desire to create disruption and chaos during the event**

Explanation 109. Correct Answer: D. Desire to create disruption and chaos during the event. Given the wide array of targets and the timing of the attacks during a major event without a clear financial motive, it's evident that the main goal of the hackers was to create widespread disruption and chaos.

Option A is incorrect. There's no indication in the scenario that data was stolen or sold, and no clear financial motive was presented.

Option B is incorrect. While ethical concerns might be a possible reason for some attacks, the scale and targets of these attacks suggest a broader motive of causing disruption.

Option C is incorrect. The scenario doesn't specify any particular focus on an athlete or team; the attacks were widespread, impacting the entire event.

Question 110. A local coffee shop offers free Wi-Fi to its customers. Recently, there have been reports of man-in-the-middle attacks on the network. The owner decides to upgrade the wireless security and wants to implement a cryptographic protocol to secure data transmissions. Which protocol would provide a balance between security and performance for the public Wi-Fi users?

- (A) **Advanced Encryption Standard (AES)**
- (B) Wired Equivalent Privacy (WEP)
- (C) RC4 Stream Cipher
- (D) Open Wireless

Explanation 110. Correct Answer: A. Advanced Encryption Standard (AES). AES offers a good balance between security and performance. It is a modern encryption standard that provides strong security without causing significant performance overhead, making it suitable for a public Wi-Fi setting where both security and user experience are important.

Option B is incorrect. WEP is an outdated encryption protocol with known vulnerabilities. It is insecure and can be easily cracked, making it unsuitable for securing a public Wi-Fi network.

Option C is incorrect. RC4 is a stream cipher that was used in older wireless protocols like WEP. It has been found to be vulnerable to various attacks and is no longer considered secure for wireless networks.

Option D is incorrect. An open wireless network does not implement any encryption, leaving data transmissions

vulnerable to eavesdropping and other attacks. It would not provide the desired security for the coffee shop's Wi-Fi users.

Question 111. TechHive Corp. is planning to sell some of its old servers. Before selling, they want to ensure that no retrievable personal or business data remains on the hard drives. Which of the following methods should TechHive use to ensure the drives are clean and the data cannot be recovered?

- (A) Simple Format
- (B) **Magnetic Wiping**
- (C) Physical Destruction
- (D) Standard Defragmentation

Explanation 111. Correct Answer: B. Magnetic Wiping.

Magnetic wiping, also known as degaussing, uses magnetic fields to permanently erase data from storage devices. It makes the data irretrievable, ensuring that personal and business data cannot be recovered even with advanced tools.

Option A is incorrect. A simple format often leaves traces of data, which can potentially be recovered using specialized software.

Option C is incorrect. While physical destruction ensures data cannot be retrieved, it would make the servers unusable for resale purposes.

Option D is incorrect. Defragmentation is a process to optimize and organize the data on a drive, but it does not erase data.

Question 112. A financial institution has reported that they experience an average of 3 phishing attacks every year that attempt to compromise their user data. Based on this data, what is the Annualized Rate of Occurrence (ARO) for these phishing attacks?

- (A) 0.33
- (B) 1
- (C) 3
- (D) 12

Explanation 112. Correct Answer: C. 3. The Annualized Rate of Occurrence (ARO) represents the expected frequency of a specific event or risk occurring each year. Given that the financial institution experiences 3 phishing attacks every year, the ARO is 3.

Option A is incorrect. An ARO of 0.33 would indicate that the event happens approximately once every three years, not thrice in a year.

Option B is incorrect. An ARO of 1 would suggest the event happens once a year, which is not consistent with the scenario.

Option D is incorrect. This would indicate the event occurs 12 times a year or once a month, which is not the case based on the information provided.

Question 113. TechFlow Corp. is undergoing a risk analysis for its online platform. If a critical vulnerability were exploited, the company would have to pay \$10,000 in repair costs, \$5,000 in compensation to customers, and a \$15,000 fine to regulatory

bodies. What would be the Single Loss Expectancy (SLE) for this vulnerability?

- (A) \$10,000
- (B) \$20,000
- (C) **\$30,000**
- (D) \$50,000

Explanation 113. Correct Answer: C. \$30,000. Single Loss Expectancy (SLE) is the cost of a single event or incident. In this scenario, adding up the repair costs, compensations, and fines gives: $\$10,000 + \$5,000 + \$15,000 = \$30,000$.

Option A is incorrect. This only accounts for the repair costs.

Option B is incorrect. This only considers the repair costs and compensations but omits the fines.

Option D is incorrect. This value exceeds the combined costs from the vulnerability being exploited.

Question 114. Country A and Country B are engaged in an ongoing territorial dispute. Suddenly, critical infrastructure facilities in Country B, such as power plants and transportation hubs, experience systematic cyberattacks. No ransom demand is made, and the attacks lead to significant disruption. What is the most probable motivation behind these cyberattacks?

- (A) Financial gain from market disruptions
- (B) Ethical hackers testing vulnerabilities
- (C) Disruption due to philosophical disagreements with Country B's policies

(D) Acts of cyberwarfare to weaken Country B's position

Explanation 114. Correct Answer: D. Acts of cyberwarfare to weaken Country B's position. Given the context of the territorial dispute and the specific targeting of critical infrastructures without any ransom demand, it's highly likely that these attacks were intended as acts of cyberwarfare by Country A or its sympathizers to exert pressure on Country B.

Option A is incorrect. While market disruptions can be exploited for financial gains, the context of a territorial dispute and the nature of the attacks suggest a motive tied to geopolitical strategy rather than financial advantage.

Option B is incorrect. Ethical hackers typically identify and report vulnerabilities rather than exploit them to cause widespread disruption.

Option C is incorrect. The attacks were too specific and large-scale to be the work of individuals or groups motivated solely by philosophical disagreements.

Question 115. The IT security team at a large corporation is evaluating monitoring tools for network traffic. They need a solution that can inspect network packets without introducing any potential latency or altering the network flow. Which type of device attribute should they consider?

- (A) Active IDS**
- (B) Passive firewall**

- (C) Active firewall
- (D) **Passive IDS**

Explanation 115. Correct Answer: D. Passive IDS. Passive IDS (Intrusion Detection System) is designed to monitor and analyze network traffic without influencing the traffic flow or causing potential latency. It observes traffic in real-time but doesn't take active actions on its own.

Option A is incorrect. An Active IDS can detect potential security breaches and take action, which may introduce latency or alter the traffic flow.

Option B is incorrect. While the term “passive firewall” is not standard, traditional firewalls can actively block or allow traffic, which can introduce changes to the network flow.

Option C is incorrect. An Active firewall actively filters network traffic based on configured policies, potentially affecting the network flow.

Question 116. In a routine security assessment, Claire found that a newly deployed database server within her organization is still using its default login credentials. Which of the following is the PRIMARY security risk associated with this finding?

- (A) The database will not function optimally
- (B) The server will need frequent patches
- (C) **Unauthorized individuals may easily gain access**
- (D) The server will consume more bandwidth

Explanation 116. Correct Answer: C. Unauthorized individuals may easily gain access. Default credentials are often publicly known, and if they are not changed, malicious actors can easily use them to gain unauthorized access to systems.

Default credentials, which may include usernames and passwords set by manufacturers for initial setup, are widely known and can be easily searched online. If not changed after deployment, they pose a significant security risk as they allow anyone with this knowledge to gain access to the system.

Option A is incorrect. The use of default credentials doesn't directly impact the optimal functioning of the database.

Option B is incorrect. The use of default credentials doesn't mean that the server will need frequent patches. However, patch management is a separate aspect of maintaining server security.

Option D is incorrect. The use of default credentials doesn't directly cause the server to consume more bandwidth.

Question 117. Mike, a network administrator, notices an unauthorized device connected directly to the company's main network switch in the server room. This device is attempting to capture network traffic. What kind of attack is this unauthorized device likely conducting?

- (A) Rogue access point
- (B) VLAN hopping
- (C) **Port mirroring**
- (D) ARP poisoning

Explanation 117. Correct Answer: C. Port mirroring. Port mirroring is a method used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port. An attacker can use this method to capture and analyze the traffic without interfering with the flow of the original packets.

Option A is incorrect. A rogue access point is a wireless access point installed on a network without the network administrator's authorization. The scenario describes a wired connection, not a wireless one.

Option B is incorrect. VLAN hopping is an attack method used to access data from different VLANs that would typically not be accessible. The scenario focuses on capturing network traffic, not crossing VLAN boundaries.

Option D is incorrect. ARP poisoning is a type of attack in which an attacker sends false ARP messages to a local network. This is not directly related to the unauthorized device connected to the switch as described.

Question 118. GreenValley Mall, located in a busy urban area, has recently faced security concerns due to the proximity of its main entrance to a major road. Which physical security enhancement can the mall management implement to create a protective barrier between the road and the entrance, ensuring pedestrian safety and preventing unauthorized vehicular access?

- (A) Reinforced Walls
- (B) Metal Detectors

- (C) **Bollards**
- (D) Perimeter Fencing

Explanation 118. Correct Answer: C. Bollards. Bollards are robust vertical posts, usually made of steel or concrete, which can be placed at specific intervals to form a protective barrier. They can effectively prevent vehicles from accessing pedestrian areas or building entrances while allowing pedestrian movement.

Option A is incorrect. While reinforced walls can offer protection against various threats, they would not be practical for separating a mall entrance from a road as they would block pedestrian access as well.

Option B is incorrect. Metal detectors are used for detecting metal objects and weapons on individuals entering a facility, not for stopping vehicular access.

Option D is incorrect. Perimeter fencing can deter unauthorized access, but it might not specifically prevent fast-moving vehicular threats like bollards do. Furthermore, a fence might not be aesthetically pleasing or practical in front of a mall entrance.

Question 119. TechCorp is implementing a new cloud-based solution. The security team has been tasked with analyzing the risks associated with this project. They've decided to categorize the risks based on their potential impact levels: Low, Medium, High, and Critical. Which type of risk analysis is TechCorp's security team employing?

- (A) Quantitative
- (B) Statistical
- (C) **Qualitative**
- (D) Financial

Explanation 119. Correct Answer: C. Qualitative. Qualitative risk analysis involves assessing risks based on descriptive categories or rankings, such as Low, Medium, High, and Critical, instead of using numeric values.

Option A is incorrect. Quantitative risk analysis involves using numerical values, often in the form of monetary figures or percentages, to evaluate risks.

Option B is incorrect. Statistical risk analysis uses statistical methods, often paired with quantitative data, to predict future risks. It doesn't categorize risks in the manner described.

Option D is incorrect. Financial risk analysis specifically evaluates risks in terms of potential financial losses and is a subset of quantitative risk analysis.

Question 120. TechBlitz Inc. recently underwent an IT audit, and one of the suggestions was to reduce the attack surface. Which of the following measures would be MOST effective in accomplishing this?

- (A) Increasing the password length requirement for all users
- (B) Implementing regular vulnerability assessments
- (C) **Deactivating unused services and ports on servers**

(D) Implementing a strict BYOD (Bring Your Own Device) policy

Explanation 120. Correct Answer: C. Deactivating unused services and ports on servers. Reducing the number of active services and ports directly diminishes the number of potential entry points for attackers, thus reducing the attack surface.

Option A is incorrect. While increasing password length improves security against brute-force attacks, it doesn't directly affect the attack surface.

Option B is incorrect. Regular vulnerability assessments identify potential security gaps, but simply identifying doesn't reduce the attack surface unless actions are taken based on findings.

Option D is incorrect. A strict BYOD policy can enhance security, but it's focused more on the types of devices and how they connect rather than reducing the number of potential attack points.

Question 121. GreenTech, a data center company, is planning to expand its operations in a region known for frequent power outages. To maintain security posture and ensure continuity of operations, which of the following should be their PRIMARY consideration regarding power?

- (A)** Using power-efficient servers to reduce electricity costs
- (B)** Setting up solar panels to promote green energy
- (C)** Investing in redundant power supplies and uninterruptible power systems (UPS)

(D) Running operations only during peak daylight hours to ensure natural lighting

Explanation 121. Correct Answer: C. Investing in redundant power supplies and uninterruptible power systems (UPS). Given the frequent power outages in the region, having redundant power supplies and UPS ensures that operations continue smoothly without abrupt interruptions, which can lead to system crashes, data corruption, or security breaches.

Option A is incorrect. While power-efficient servers can reduce costs, they do not address the primary concern of power outages and maintaining operations.

Option B is incorrect. Solar panels promote green energy but might not provide consistent and immediate power backup during outages, especially during nighttime or cloudy days.

Option D is incorrect. Limiting operations to daylight hours is not a practical solution for a data center, as it restricts operational capacity and doesn't directly address the issue of power outages.

Question 122. WebFlix, a popular online movie streaming service, experienced a data center outage due to a natural disaster. They had backups in place and restored their systems using data from 6 hours prior to the outage. This resulted in the loss of some user interactions, like ratings and watchlists from the last 6 hours. What term describes the 6-hour gap between the last backup and the time of the outage?

- (A) Recovery Time Objective (RTO)
- (B) Maximum Tolerable Downtime (MTD)
- (C) Recovery Duration Period (RDP)
- (D) **Recovery Point Objective (RPO)**

Explanation 122. Correct Answer: D. Recovery Point Objective (RPO). The Recovery Point Objective (RPO) is the maximum acceptable amount of data loss measured in time. For WebFlix, this means they could afford to lose up to 6 hours of data (user interactions in this case) in the event of a disaster.

Option A is incorrect. Recovery Time Objective (RTO) is the maximum acceptable amount of time that a system can be down after a disruption.

Option B is incorrect. Maximum Tolerable Downtime (MTD) represents the total amount of time a system can afford to be non-operational without incurring significant risks or significant losses.

Option C is incorrect. Recovery Duration Period (RDP) is not a standard term in business continuity and disaster recovery planning.

Question 123. Jane, the CISO at a financial institution, is overseeing the decommissioning of several old servers. She is aware that while some data must be destroyed, other data must be retained due to industry regulations. Which principle should Jane primarily focus on to ensure compliance?

- (A) Minimum necessary principle
- (B) Principle of least privilege

- (C) **Data retention policy**
- (D) Mandatory vacation policy

Explanation 123. Correct Answer: C. Data retention policy.

A data retention policy specifically defines how long data should be retained and the manner of its storage based on business needs, regulatory requirements, and other factors. In the context of decommissioning servers, adhering to this policy will ensure that Jane complies with regulations related to data retention.

Option A is incorrect. The minimum necessary principle pertains to healthcare and refers to only using, disclosing, or requesting the amount of information necessary to accomplish a specific task.

Option B is incorrect. The principle of least privilege pertains to access controls and means giving users the minimum levels of access necessary to perform their jobs.

Option D is incorrect. A mandatory vacation policy pertains to ensuring employees take time off so that potential fraudulent activities might be detected in their absence. It doesn't directly address data retention.

Question 124. A medium-sized e-commerce company recently experienced a data breach due to an external attack. Post-incident analysis revealed that while there were indications of the attack in their network traffic, no alarms were raised at the time of the attack. The company now wants to implement a solution to actively monitor and take action against malicious

network traffic. Which of the following should they deploy?

- (A) Intrusion Detection System (IDS)
- (B) Network Access Control (NAC)
- (C) Proxy server
- (D) **Intrusion Prevention System (IPS)**

Explanation 124. Correct Answer: D. Intrusion Prevention System (IPS). An Intrusion Prevention System (IPS) not only detects malicious network activities but also takes active steps to prevent or block them, which is ideal for a company looking to bolster its defenses against real-time threats.

Option A is incorrect. An Intrusion Detection System (IDS) will detect and alert on malicious activity but does not take active steps to prevent the threat.

Option B is incorrect. Network Access Control (NAC) is primarily used for controlling network access based on policies, not for active monitoring and prevention of malicious network traffic.

Option C is incorrect. A Proxy server acts as an intermediary for requests from clients seeking resources but is not specifically designed to detect or prevent intrusions.

Question 125. A cybersecurity analyst at XYZ Corp is looking to deploy a system that appears to be vulnerable and enticing to attackers. The main goal is to study the tactics, techniques, and procedures (TTPs) of potential adversaries, without them realizing that they're interacting with a decoy. Which of the following would BEST meet this requirement?

- (A) Intrusion Detection System (IDS)
- (B) Firewall
- (C) **Honeypot**
- (D) VPN Concentrator

Explanation 125. Correct Answer: C. Honeypot. A honeypot is a security mechanism designed to lure attackers into interacting with a seemingly vulnerable system. Its primary purpose is not to block or prevent attacks but to log and study them. By analyzing the activities on the honeypot, security professionals can gain insights into the methods and motivations of the attackers.

Option A is incorrect. An Intrusion Detection System (IDS) is designed to detect malicious activities on a network and alert administrators. While it can identify threats, it doesn't actively lure attackers.

Option B is incorrect. A firewall is designed to block or allow traffic based on specific rules. It doesn't present itself as a vulnerable target to lure attackers.

Option D is incorrect. A VPN Concentrator is a device that provides remote access to a network over a secure connection. Its primary purpose is to enable secure remote access, not to act as a decoy for attackers.

Question 126. The networking team at SecureNet Corp. is setting up a new branch office. They want to ensure secure connectivity between the branch office and the main office. Which of the following would BEST provide this?

- (A) Establishing a clear line of sight for wireless antennas between the two locations
- (B) Implementing a Virtual Private Network (VPN) between the two sites**
- (C) Increasing bandwidth on the public internet connection at both locations
- (D) Using multi-factor authentication for all user accounts in both locations

Explanation 126. Correct Answer: B. Implementing a Virtual Private Network (VPN) between the two sites. VPNs provide secure, encrypted connections over potentially insecure networks, such as the internet, making them ideal for securely connecting remote locations.

Option A is incorrect. While a clear line of sight might facilitate wireless communication, it doesn't inherently provide secure connectivity.

Option C is incorrect. Increasing bandwidth enhances data transfer rates but doesn't inherently secure the connection between sites.

Option D is incorrect. Multi-factor authentication is a robust security measure for user access but doesn't secure network connectivity between sites.

Question 127. TechVault, a company specializing in secure storage solutions, recently had an unauthorized intrusion where a burglar managed to bypass their motion sensors. In a bid to prevent future breaches, they are considering deploying a

system that can detect weight changes in a restricted floor area to alert any unauthorized access. Which of the following would be BEST for this requirement?

- (A) Ultrasonic motion detectors
- (B) **Pressure-sensitive floor mats**
- (C) CCTV cameras with facial recognition
- (D) Glass break sensors

Explanation 127. Correct Answer: B. Pressure-sensitive floor mats. Pressure-sensitive floor mats are designed to detect weight changes or pressure when stepped on. This makes them an effective solution for monitoring restricted areas and alerting unauthorized access based on weight detection.

Option A is incorrect. Ultrasonic motion detectors use sound waves to detect motion in an area but do not measure weight or pressure.

Option C is incorrect. CCTV cameras with facial recognition provide visual surveillance and can identify individuals, but they don't detect weight changes on the floor.

Option D is incorrect. Glass break sensors detect the sound of breaking glass and are primarily used for windows and glass doors, not for detecting pressure or weight changes on a floor.

Question 128. SafeMed, a medical facility, uses a life-saving medical device with embedded software. Recently, a security vulnerability was found in the software, but due to the device's FDA regulatory status and the software's design, it cannot be patched immediately. How should SafeMed address the security

concerns related to this device?

- (A) Disconnect the device from all networks and only use it in standalone mode
- (B) Inform patients about the vulnerability and let them decide whether to use the device
- (C) **Implement network segmentation and strictly control access to the device**
- (D) Return the device to the manufacturer for a full refund

Explanation 128. Correct Answer: C. Implement network segmentation and strictly control access to the device. By implementing network segmentation, SafeMed can isolate the vulnerable device from other parts of the network, reducing the risk of potential exploitation. Strictly controlling access ensures only authorized personnel can use or interact with the device.

Option A is incorrect. Completely disconnecting the device might limit its functionality, especially if it needs network access for updates, data transfer, or other essential operations.

Option B is incorrect. While transparency is important, simply informing patients without taking protective measures may not be enough to ensure safety and could lead to panic or misinformation.

Option D is incorrect. Returning the device might not be feasible, especially if there are no immediate replacements available, and it is vital for patient care.

Question 129. The network administrator at a university wants to ensure that when students log onto the campus wireless

network, their credentials are verified by the university's central authentication server. Additionally, the administrator wants to make sure that the data between the wireless access point and the central server is encrypted. Which solution should the administrator implement?

- (A) WPA3 with SAE
- (B) WPA2-Personal with AES
- (C) **WPA2-Enterprise with RADIUS**
- (D) Open wireless with VPN

Explanation 129. Correct Answer: C. WPA2-Enterprise with RADIUS. WPA2-Enterprise provides a more robust authentication method suitable for larger organizations like universities. By using RADIUS, the university can centralize the authentication process, ensuring students' credentials are verified against the central server. RADIUS also encrypts the data between the wireless access point and the central server, providing an additional layer of security.

Option A is incorrect. WPA3 with SAE is primarily used for secure handshakes between devices and does not directly relate to centralized authentication against a server like RADIUS.

Option B is incorrect. WPA2-Personal with AES is designed for personal or small office use where a pre-shared key is used. It doesn't support centralized authentication like RADIUS.

Option D is incorrect. While a VPN can encrypt data between a device and a network, it doesn't centralize wireless authentication in the way that RADIUS does with WPA2-Enterprise.

Question 130. TechHaus has recently experienced multiple security breaches where unauthorized personnel have managed to infiltrate their server rooms after hours. To enhance security measures, the company decided to deploy a new system. Which of the following options would BEST detect human intruders based on their body heat even in complete darkness?

- (A) Installing CCTV cameras with LED lights
- (B) Using ultrasonic motion sensors
- (C) **Deploying infrared (IR) sensors**
- (D) Implementing RFID badge readers at the entrance

Explanation 130. Correct Answer: C. Deploying infrared (IR) sensors. Infrared (IR) sensors detect infrared radiation, such as the heat emitted by the human body. This makes them particularly effective in detecting human intruders, even in complete darkness, based on the body heat they emit.

Option A is incorrect. While CCTV cameras with LED lights can provide visual surveillance, they rely on light to produce images and may not detect intruders in complete darkness as efficiently as infrared sensors.

Option B is incorrect. Ultrasonic motion sensors detect movement through sound waves, not body heat, making them less efficient in differentiating between a human intruder and other moving objects.

Option D is incorrect. RFID badge readers control access at entry points but do not detect human intruders based on their body heat inside a facility.

Question 131. SecureTech Corp, a company dealing with sensitive client data, is redesigning its main office entrance to enhance security. They want to ensure that only one person gains access at a time, even if multiple people try to enter using a single authorized access badge. Which of the following would best serve this purpose?

- (A) CCTV Cameras
- (B) **Mantrap**
- (C) Biometric Scanners
- (D) Motion Detectors

Explanation 131. Correct Answer: B. Mantrap. A mantrap, also known as an access control vestibule, is a physical security access control system comprising a small space with two sets of interlocking doors. The first door must close before the second door opens, ensuring that only one person can pass through at a time. This design prevents tailgating or piggybacking, where unauthorized individuals attempt to enter a secure area by following closely behind an authorized individual.

Option A is incorrect. While CCTV cameras monitor and record activities, they do not physically prevent multiple people from entering at once using a single access badge.

Option C is incorrect. Biometric scanners provide a means of authenticating individuals based on unique physical or behavioral characteristics, but they do not prevent tailgating on their own.

Option D is incorrect. Motion detectors can detect movement but do not restrict the entry of multiple individuals trying to use a single authorized access badge.

Question 132. An enterprise wants to configure its firewall so that if a malfunction occurs, the firewall should automatically allow traffic to ensure business continuity. Which failure mode should be implemented?

- (A) Fail-safe
- (B) Fail-over
- (C) Fail-closed
- (D) **Fail-open**

Explanation 132. Correct Answer: D. Fail-open. In a fail-open mode, when the system or device fails, it defaults to an “open” state, allowing traffic to pass through. This mode prioritizes availability over strict security.

Option A is incorrect. “Fail-safe” is a term that typically refers to a system’s ability to default to a safe condition in case of a failure. However, in the context of firewalls and access control systems, “fail-open” or “fail-closed” are the preferred terms.

Option B is incorrect. “Fail-over” refers to switching to a backup system or component in the event of a failure. It doesn’t describe the behavior of allowing or denying traffic during a failure.

Option C is incorrect. Fail-closed means that when a malfunction occurs, the system would block all traffic by default, which is the opposite of what the enterprise wants.

Question 133. During a board meeting at DataFlow Corp., the CEO emphasizes that while they are willing to take certain risks for innovation, there's a limit to the amount of risk they are willing to take, especially concerning potential financial losses. To ensure that risks stay below this level, what should be defined in the risk register?

- (A) Risk Owner Assignment
- (B) Key Risk Indicator (KRI)
- (C) Risk Impact Analysis
- (D) **Risk Threshold**

Explanation 133. Correct Answer: D. Risk Threshold. The risk threshold indicates the maximum level of risk an organization is willing to tolerate or accept. Setting a clear risk threshold ensures that any risks that surpass this level are given priority for management or mitigation.

Option A is incorrect. While assigning a Risk Owner is crucial for accountability, it doesn't define the maximum level of risk an organization is willing to tolerate.

Option B is incorrect. A Key Risk Indicator (KRI) provides early signals of increasing risk exposures. While they are essential for monitoring risks, they don't establish the maximum tolerable risk level.

Option C is incorrect. Risk Impact Analysis assesses the potential consequences of a given risk but doesn't set a level indicating the maximum risk the organization is prepared to accept.

Question 134. A healthcare provider is updating its network infrastructure. Due to the sensitive nature of the medical data they handle, they want to ensure that any anomalies or malicious activities in the network are immediately detected and alerted. Which system should they primarily consider?

- (A) Intrusion Prevention System (IPS)
- (B) **Intrusion Detection System (IDS)**
- (C) DHCP server
- (D) VPN concentrator

Explanation 134. Correct Answer: B. Intrusion Detection System (IDS). An Intrusion Detection System (IDS) actively monitors network traffic for any signs of malicious activities or policy violations and alerts the administrators. It is suitable for organizations that want to ensure anomalies are promptly detected.

Option A is incorrect. An Intrusion Prevention System (IPS) does actively monitor and detect malicious traffic but also takes measures to prevent it. While an IPS could be beneficial for the healthcare provider, the primary requirement mentioned was for detection and alerting, which is the primary function of an IDS.

Option C is incorrect. A DHCP (Dynamic Host Configuration Protocol) server assigns IP addresses to devices in a network. It does not monitor or alert on malicious network activities.

Option D is incorrect. A VPN concentrator is used to create and manage VPN connections, providing secure access to a network, but it doesn't primarily detect intrusions.

Question 135. BioGen Inc., a biotechnology company, has implemented a layered security approach. They are considering adding a human element to their security measures for their research labs. Which of the following would best provide the ability to evaluate and respond to various security situations with human judgment?

- (A) Installing biometric locks
- (B) **Employing security guards**
- (C) Implementing an access control vestibule
- (D) Deploying AI-driven security cameras

Explanation 135. Correct Answer: B. Employing security guards. Security guards provide the advantage of human judgment and can evaluate, respond, and adapt to a wide variety of security situations, making them ideal for adding a human element to a layered security approach.

Option A is incorrect. While biometric locks can control access based on unique human features, they don't provide the evaluation and response capabilities of a human guard.

Option C is incorrect. An access control vestibule controls access into an area, often with two sets of doors, but it does not provide the evaluation, judgment, or immediate response that a security guard does.

Option D is incorrect. While AI-driven security cameras can provide advanced monitoring and potentially detect suspicious activities, they don't replace the judgment and immediate response capabilities of a human security guard.

Question 136. ExamsDigest Corp, a technology company, recently conducted a security assessment to align with industry best practices. The company's current security posture was compared to its desired future state, revealing discrepancies. Which of the following best describes the approach ExamsDigest Corp employed?

- (A) Vulnerability Assessment
- (B) Penetration Testing
- (C) **Gap Analysis**
- (D) Threat Modeling

Explanation 136. Correct Answer: C. Gap Analysis. Gap analysis is a method of comparing the current state of something (such as security measures) with a future desired state to identify the discrepancies or “gaps”. In the scenario, ExamsDigest Corp compared their current security posture to a desired future state, which is consistent with the process of gap analysis.

Option A is incorrect. A vulnerability assessment focuses on identifying, quantifying, and ranking vulnerabilities in a system, not comparing the current state with a desired future state.

Option B is incorrect. Penetration testing is an authorized simulated cyberattack on a system to evaluate its security, not to compare its current state with a desired future state.

Option D is incorrect. Threat modeling is the process of identifying potential threats to a system and determining the risk they pose, not comparing the current state with a desired future state.

Question 137. Sophia, the CFO of a medium-sized company, received a call from an individual claiming to be from the IT department. The caller requested her login details for a “critical system update.” Suspecting something wasn’t right, Sophia hung up and contacted her IT department, which confirmed no such call was made by them. Which type of attack did Sophia most likely experience?

- (A) **Vishing**
- (B) Phishing
- (C) SQL Injection
- (D) Cross-Site Request Forgery (CSRF)

Explanation 137. Correct Answer: A. Vishing. Vishing, or voice phishing, is an attack where fraudsters use the telephone to mislead individuals into revealing personal information or login credentials.

Option B is incorrect. Phishing is typically an attempt to obtain sensitive information through deceptive emails and websites, not voice calls.

Option C is incorrect. SQL Injection is an attack type that tries to execute malicious SQL statements in a database. It is not related to voice calls.

Option D is incorrect. Cross-Site Request Forgery (CSRF) is a type of attack where the attacker tricks the victim into submitting a malicious request. This is unrelated to voice call scenarios.

Question 138. A medium-sized enterprise is preparing to upgrade its office workstations. The IT department is considering purchasing devices from a lesser-known, but cheaper, vendor. Which of the following should be the PRIMARY consideration before finalizing the acquisition?

- (A) Whether the vendor offers a longer warranty period
- (B) The aesthetics and design of the workstations
- (C) **The vendor's adherence to industry security standards and practices**
- (D) The amount of training required for IT staff to support the new devices

Explanation 138. Correct Answer: C. The vendor's adherence to industry security standards and practices.

Ensuring that the vendor adheres to industry security standards and practices is critical for maintaining a secure environment. Devices that don't meet security standards could introduce vulnerabilities into the organization.

Option A is incorrect. While a longer warranty period might be attractive, it should not be the primary concern over security considerations.

Option B is incorrect. Aesthetics and design, while potentially important for branding or user satisfaction, are not as critical as security considerations.

Option D is incorrect. Training the IT staff is important, but it shouldn't take precedence over ensuring the devices themselves are secure.

Question 139. An employee of XYZ Corp downloaded a seemingly benign PDF file from a vendor's website. After opening the PDF, the company's intrusion detection system (IDS) alerted the security team about suspicious activity originating from the employee's computer. The PDF file most likely contained which of the following threats?

- (A) Watering Hole Attack
- (B) **Malicious Macro**
- (C) SQL Injection
- (D) Credential Harvesting

Explanation 139. Correct Answer: B. Malicious Macro.

Many document types, including PDFs, can contain macros. A malicious macro can execute unwanted actions, such as downloading and installing malware, when the document is opened.

Option A is incorrect. A Watering Hole Attack is when an attacker guesses or observes which websites an organization often uses and infects them with malware, with the intent of compromising members of that organization. The scenario does not provide evidence pointing to this kind of attack.

Option C is incorrect. SQL Injection is a type of attack that aims to execute malicious SQL statements in a database. This type of attack is unrelated to opening a PDF file.

Option D is incorrect. A Drive-By Download involves automatically downloading software, often malicious, without user knowledge or consent, typically when a user visits a

compromised website. The scenario specifically discusses a downloaded and then manually opened PDF.

Question 140. A rapidly growing e-commerce platform has been facing intermittent downtimes, especially during sale events. To ensure high availability and even distribution of traffic among servers, the company is considering deploying a specific type of network appliance. Which of the following should the company deploy?

- (A) Intrusion Detection System (IDS)
- (B) VPN concentrator
- (C) **Load balancer**
- (D) Proxy server

Explanation 140. Correct Answer: C. Load balancer. A load balancer is designed to distribute incoming network traffic across multiple servers to ensure that no single server is overwhelmed with too much traffic. This helps in ensuring high availability and optimizing resource utilization.

Option A is incorrect. An Intrusion Detection System (IDS) is primarily used for detecting malicious activities in the network, not for distributing traffic among servers.

Option B is incorrect. A VPN concentrator is used to create and manage VPN connections, not for balancing load among servers.

Option D is incorrect. While a proxy server can distribute client requests to different servers, its primary role is to act as

an intermediary, not to ensure high availability or evenly distribute traffic.

Question 141. TechFusion Inc. is a well-established technology company that has been in the market for over 15 years.

Recently, the board of directors decided that the company will pursue aggressive growth strategies by entering new, untested markets and launching cutting-edge products, even if these strategies come with significant risks. How would you classify TechFusion Inc.'s risk appetite?

- (A) Conservative
- (B) **Expansionary**
- (C) Neutral
- (D) Risk-averse

Explanation 141. Correct Answer: B. Expansionary.

Expansionary risk appetite is characterized by an entity's willingness to accept a higher level of risk in pursuit of higher rewards. Given that TechFusion Inc. is looking to enter new markets and launch cutting-edge products, which inherently come with significant risks, their risk appetite can be classified as expansionary.

Option A is incorrect. A conservative risk appetite means an organization is very cautious and avoids taking significant risks, which is the opposite of TechFusion Inc.'s approach.

Option C is incorrect. Neutral risk appetite means an organization neither seeks to take on nor avoid risk, maintaining its current risk position.

Option D is incorrect. Risk-averse is similar to conservative, where an organization is very cautious about taking on new risks. It doesn't capture the aggressive growth strategy described.

Question 142. Alex, an employee at XYZ Corp, noticed an unfamiliar USB drive lying in the company parking lot. Out of curiosity, Alex plugged the device into his workstation. Almost immediately, his antivirus program detected malicious software trying to execute. What type of attack did Alex likely encounter?

- (A) Man-in-the-Middle Attack
- (B) Evil Twin
- (C) Spear Phishing
- (D) **USB Drop Attack**

Explanation 142. Correct Answer: D. USB Drop Attack. A USB Drop Attack involves leaving malware-infected removable devices, such as USB drives, in places where they can be found and used by unsuspecting individuals. Once the device is plugged into a computer, it can potentially execute malicious software or scripts.

Option A is incorrect. A Man-in-the-Middle Attack involves an attacker secretly intercepting and possibly altering the communication between two parties without them noticing. It is not related to USB devices.

Option B is incorrect. Evil Twin refers to a rogue Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications. It doesn't pertain to USB devices.

Option C is incorrect. Spear Phishing is a targeted attempt to steal sensitive information through deceptive emails directed at specific individuals or companies. It is not associated with USB devices.

Question 143. A rapidly growing e-commerce company has recently experienced an increase in cross-site scripting (XSS) and SQL injection attacks. The company wants to deploy a solution that specifically protects against these threats at the application layer. Which type of firewall would be most appropriate?

- (A) Stateful Packet Inspection Firewall
- (B) Proxy Firewall
- (C) Network Layer Firewall
- (D) **Web Application Firewall (WAF)**

Explanation 143. Correct Answer: D. Web Application Firewall (WAF). A Web Application Firewall (WAF) is specifically designed to protect web applications by monitoring, filtering, and blocking potentially harmful HTTP traffic. This includes protection against threats like XSS and SQL injection attacks that are common against web applications.

Option A is incorrect. While a Stateful Packet Inspection Firewall can monitor the state of active connections and make decisions based on the context of the traffic, it doesn't specifically address application layer vulnerabilities like XSS and SQL injection.

Option B is incorrect. Although a Proxy Firewall can provide some application layer filtering, its primary purpose is not

tailored to protect against specific web application vulnerabilities.

Option C is incorrect. A Network Layer Firewall primarily operates at the network layer and won't provide specialized protection against application layer threats.

Question 144. A financial institution wants to enhance the security of its wired network. The goal is to ensure that only authorized devices can connect to the network, and the authentication process should be based on credentials or digital certificates. Which of the following protocols would best serve this purpose?

- (A) SNMPv3
- (B) SSL/TLS
- (C) **802.1X EAP**
- (D) DHCP

Explanation 144. Correct Answer: C. 802.1X EAP. 802.1X Extensible Authentication Protocol (EAP) provides port-based network access control and is used on wired networks to ensure that only authenticated devices can connect. It supports multiple authentication methods including credentials, digital certificates, and smart cards.

Option A is incorrect. SNMPv3 (Simple Network Management Protocol version 3) is used for network management and monitoring, not for port-based network access control.

Option B is incorrect. SSL/TLS (Secure Sockets Layer/Transport Layer Security) is a protocol used for securing data

transmission on the internet, not for port-based network access control.

Option D is incorrect. DHCP (Dynamic Host Configuration Protocol) assigns IP addresses to devices on a network but doesn't deal with port-based authentication.

Question 145. An organization is evaluating different security solutions for their new branch office. They want to ensure that the chosen solution can be rapidly deployed with minimal configuration. Which of the following options BEST fulfills this requirement?

- (A) A customized Intrusion Prevention System (IPS) tailored to the organization's unique needs
- (B) **A zero-touch provisioning firewall**
- (C) An open-source firewall with extensive manual settings
- (D) A security information and event management (SIEM) solution requiring manual log source integration

Explanation 145. Correct Answer: B. A zero-touch provisioning firewall. Zero-touch provisioning allows devices to be provisioned and configured automatically, ensuring rapid deployment with minimal manual intervention.

Option A is incorrect. While a customized IPS might be tailored for the organization's needs, it often requires a lot of configuration and isn't the fastest to deploy.

Option C is incorrect. Open-source firewalls that require extensive manual settings are not considered rapid to deploy as they necessitate more time for configuration.

Option D is incorrect. A SIEM solution that requires manual log source integration would not be the quickest to deploy due to the manual steps involved.

Question 146. A company named TechFlow is planning to produce a new line of smart home devices. They have opted to use a single supplier for a crucial component in their devices. Which of the following represents the MOST significant security risk associated with this decision?

- (A) It will be challenging to negotiate prices with just one supplier
- (B) If the supplier's delivery timeline is delayed, product launch might be postponed
- (C) **A compromise at the supplier could lead to vulnerabilities in all devices**
- (D) TechFlow will need to rely on the supplier's warranty and return policies

Explanation 146. Correct Answer: C. A compromise at the supplier could lead to vulnerabilities in all devices. Relying on a single supplier means that any security issues at that supplier's end might translate directly into vulnerabilities in every device using that component.

In a supply chain, the security of every entity is paramount. If one supplier gets compromised, and the company relies solely on that supplier for a crucial component, every product using

that component might be vulnerable. This could have widespread implications for the security of the end-users and damage the company's reputation.

Option A is incorrect. Price negotiation is a business concern and not directly related to the security implications of using a single supplier.

Option B is incorrect. While delivery delays can have business implications, they don't represent a direct security risk.

Option D is incorrect. Warranty and return policies are operational considerations but aren't the primary security risks associated with relying on a single supplier.

Question 147. The security team of a multinational company deployed a network of honeypots globally, making it appear as an interconnected and realistic environment. They aim to study coordinated multi-stage attacks. This deceptive setup is known as:

- (A) Firewall Cluster
- (B) Virtual LAN (VLAN)
- (C) Distributed Denial of Service (DDoS) Prevention
- (D) **Honeynet**

Explanation 147. Correct Answer: D. Honeynet. A honeynet is essentially a network of honeypots. It is designed to be attractive to attackers, making them believe they are attacking a real network, while in reality, they are being observed, and their tactics and techniques are being analyzed.

Option A is incorrect. A Firewall Cluster is a group of firewalls operating together to increase reliability and performance. It doesn't serve as a decoy to attract attackers.

Option B is incorrect. A Virtual LAN (VLAN) is a network protocol used to create logically segmented networks within a physical network, improving performance and security. It's not a decoy system.

Option C is incorrect. Distributed Denial of Service (DDoS) Prevention solutions focus on identifying and mitigating large-scale attempts to disrupt network service availability. They do not present a deceptive environment for attackers.

Question 148. David, an IT administrator, noticed an unusually high data usage on several company-owned mobile devices even when they are connected to the corporate Wi-Fi. He suspects these devices might be using cellular data in the background. Which of the following solutions should David implement to ensure that company devices use only the corporate Wi-Fi for data transactions when they're in the office?

- (A) Enable Airplane mode on all devices
- (B) Set up a Wi-Fi whitelist
- (C) **Implement a mobile device management (MDM) policy to prioritize Wi-Fi**
- (D) Disable cellular antennas in the office area

Explanation 148. Correct Answer: C. Implement a mobile device management (MDM) policy to prioritize Wi-Fi. An MDM solution allows administrators to enforce policies on mobile devices. By implementing a policy that prioritizes Wi-Fi

connections, David can ensure that company devices will use the corporate Wi-Fi network when available, thus reducing cellular data usage.

Option A is incorrect. While enabling Airplane mode would cut off cellular data, it would also disable all other forms of communication including Wi-Fi, making the device unusable for its intended purposes.

Option B is incorrect. Setting up a Wi-Fi whitelist does not prevent a device from using cellular data. It only restricts which Wi-Fi networks a device can connect to.

Option D is incorrect. Disabling cellular antennas is a drastic measure that could affect other devices and services in the vicinity. It's also impractical and potentially illegal depending on local regulations.

Question 149. A university is looking to revamp its wireless network to provide secure access for students and faculty. The IT department wants an authentication method that leverages a centralized server to validate user credentials and can integrate with their existing directory service. Which authentication protocol should they consider?

- (A) Pre-shared Key (PSK)
- (B) Lightweight Extensible Authentication Protocol (LEAP)
- (C) Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- (D) Shared Secret Challenge

Explanation 149. Correct Answer: C. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). EAP-TLS provides strong security by using digital certificates to authenticate both the client and the server. It operates in conjunction with a RADIUS server, allowing for centralized management of user credentials and seamless integration with existing directory services.

Option A is incorrect. Pre-shared Key (PSK) does not involve a centralized server for authentication. Instead, a single shared key is used for all devices, which may not be scalable or secure for a large university setting.

Option B is incorrect. While LEAP provides centralized authentication via a RADIUS server, it has known vulnerabilities and may not offer the level of security the university is looking for.

Option D is incorrect. Shared Secret Challenge is not a standard wireless authentication protocol. In practice, challenges based on shared secrets (like PSK) can be vulnerable if the secret becomes known.

Question 150. A university is looking to revamp its wireless network to provide secure access for students and faculty. The IT department wants an authentication method that leverages a centralized server to validate user credentials and can integrate with their existing directory service. Which authentication protocol should they consider?

- (A) Pre-shared Key (PSK)
- (B) Lightweight Extensible Authentication Protocol

(LEAP)

(C) **Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)**

(D) Shared Secret Challenge

Explanation 150. Correct Answer: C. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). EAP-TLS provides strong security by using digital certificates to authenticate both the client and the server. It operates in conjunction with a RADIUS server, allowing for centralized management of user credentials and seamless integration with existing directory services.

Option A is incorrect. Pre-shared Key (PSK) does not involve a centralized server for authentication. Instead, a single shared key is used for all devices, which may not be scalable or secure for a large university setting.

Option B is incorrect. While LEAP provides centralized authentication via a RADIUS server, it has known vulnerabilities and may not offer the level of security the university is looking for.

Option D is incorrect. Shared Secret Challenge is not a standard wireless authentication protocol. In practice, challenges based on shared secrets (like PSK) can be vulnerable if the secret becomes known.

Question 151. CyberGuard LLC, a cybersecurity firm, is in a stable position in its industry with consistent returns. The leadership decides not to pursue aggressive growth strategies

but instead chooses to maintain its current market share and operational scale. They are open to minor risks but avoid major disruptions. How can one best describe CyberGuard LLC's risk appetite?

- (A) Expansionary
- (B) **Neutral**
- (C) Conservative
- (D) Aggressive

Explanation 151. Correct Answer: B. Neutral. A neutral risk appetite means an organization is neither aggressively pursuing risks for high rewards nor entirely avoiding them. Given that CyberGuard LLC is looking to maintain its current position and is open to minor risks, their risk appetite can be classified as neutral.

Option A is incorrect. Expansionary risk appetite denotes an organization's willingness to accept higher risks to achieve potentially higher rewards, which doesn't align with CyberGuard LLC's strategy.

Option C is incorrect. While CyberGuard LLC is cautious, their stance is not entirely against taking risks. A conservative appetite would imply they avoid most risks, but they are open to minor ones.

Option D is incorrect. Aggressive would imply a strong willingness to take on significant risks, which is not the stance described for CyberGuard LLC.

Question 152. After a series of cyber-attacks on a company's infrastructure, the IT team decided to deploy a solution that would seem like a legitimate part of their network but is intentionally isolated and monitored. They intend to detect and analyze malicious activities in this isolated environment. What technology are they most likely implementing?

- (A) Network segmentation
- (B) **Honeypot**
- (C) DMZ (Demilitarized Zone)
- (D) Sandboxing

Explanation 152. Correct Answer: B. Honeypot. A honeypot is intentionally set up to appear as a legitimate part of a network, but it is isolated and closely monitored. Its purpose is to attract attackers and observe their actions, thereby providing insights into potential threats and the methods employed by adversaries.

Option A is incorrect. Network segmentation involves dividing a network into smaller sub-networks. While this can enhance security by limiting attackers' access to specific segments, it doesn't act as a decoy to attract attackers.

Option C is incorrect. A DMZ (Demilitarized Zone) is a subnet that acts as a buffer between the internet and an organization's internal network. While it can contain servers accessible to external users, its primary purpose is not to act as a decoy but to provide a layer of protection.

Option D is incorrect. Sandboxing is a security mechanism that allows programs to run in a separate environment to

prevent them from affecting the broader system. It's used for testing and analyzing potentially malicious software, not for luring attackers.

Question 153. Your organization is considering a partnership with TechVendor Inc., a software solution provider. Before finalizing the agreement, you wish to ensure their application's security. What would be the most direct method to assess the robustness of their system against potential cyber threats?

- (A) Conducting an internal security awareness training
- (B) Reviewing their past audit reports
- (C) Implementing strict firewall rules
- (D) **Performing a penetration test on their application.**

Explanation 153. Correct Answer: D. Performing a penetration test on their application. Penetration testing is a proactive method used to evaluate the security of an application by simulating an attack from malicious outsiders or insiders. It provides a direct measure of the vulnerabilities present in the application that could potentially be exploited by an attacker.

Option A is incorrect. While security awareness training is crucial for educating staff about security best practices, it does not directly assess the security of an external vendor's application.

Option B is incorrect. Past audit reports can provide valuable insights into a vendor's security posture, but they do not offer real-time assessment like penetration testing.

Option C is incorrect. Implementing firewall rules is a protective measure, but it does not evaluate the current security of the vendor's application.

Question 154. An e-commerce platform recently suffered a data breach where attackers exploited cookies to impersonate user sessions. A security analyst is tasked with recommending measures to secure user cookies. Which of the following measures will ensure that cookies are transmitted securely between the user's browser and the server?

- (A) Storing cookies in the database
- (B) **Implementing the "Secure" attribute for cookies**
- (C) Increasing the cookie expiration time
- (D) Base64 encoding the cookie content

Explanation 154. Correct Answer: B. Implementing the "Secure" attribute for cookies. The "Secure" attribute ensures that a cookie is only sent over secure, encrypted HTTPS connections. By implementing this attribute, the cookie won't be transmitted over unencrypted HTTP connections, reducing the risk of interception by malicious actors.

Option A is incorrect. Storing cookies in the database doesn't necessarily secure the transmission of cookies between the client and server. It's more about storage security rather than transmission security.

Option C is incorrect. Increasing the cookie expiration time can actually increase the window of opportunity for an attacker to exploit a cookie, making it a less secure practice.

Option D is incorrect. Base64 encoding is not encryption; it's just a way to represent binary data in an ASCII string format. Encoding can be easily reversed, offering little to no security.

Question 155. An organization has recently received a new software patch for its critical infrastructure. Before deploying it to production, the security team wants to understand its behavior and ensure it doesn't contain any malicious code. Which of the following methods would be MOST effective for safely executing and observing the patch's behavior?

- (A) Deploying the patch during a maintenance window
- (B) **Running the patch within a sandbox environment**
- (C) Conducting a code review of the patch
- (D) Installing the patch on a virtual machine

Explanation 155. Correct Answer: B. Running the patch within a sandbox environment. Running the patch within a sandbox environment allows the security team to execute and observe the software's behavior in an isolated environment, ensuring it doesn't interfere with or harm the actual production environment.

Option A is incorrect. Deploying the patch during a maintenance window reduces operational disruptions but doesn't allow for safe observation of the patch's behavior.

Option C is incorrect. While a code review can identify potential security concerns in the patch, it may not reveal the actual behavior when executed.

Option D is incorrect. Installing the patch on a virtual machine is a form of isolation, but a sandbox provides a more controlled and restrictive environment specifically designed for observing software behavior.

Question 156. A recently hired security analyst at CyberTech Inc. wants to get a better understanding of the organization's network infrastructure. Which of the following activities would provide a LIST of servers, workstations, printers, switches, and routers currently active in the network?

- (A) Vulnerability Scanning
- (B) Intrusion Detection
- (C) **Network Enumeration**
- (D) Penetration Testing

Explanation 156. Correct Answer: C. Network

Enumeration. Network enumeration is the process of identifying devices on a network. Through enumeration, an analyst can gather information about network devices, their types, and other attributes, thereby getting a clearer picture of the network's infrastructure.

Option A is incorrect. Vulnerability scanning aims to identify vulnerabilities in network devices and systems, not necessarily to list all active devices.

Option B is incorrect. Intrusion detection focuses on monitoring network traffic for malicious activities and potential security breaches.

Option D is incorrect. Penetration testing aims to exploit vulnerabilities in a network to determine its security posture, not to list all active devices.

Question 157. Tech Enterprises is planning to release a new product. As part of the product's creation, they've sourced components from various vendors. The security team is tasked with assessing risks linked to the supply chain. Which of the following is the MOST concerning risk when sourcing components from multiple vendors?

- (A) Difficulty in tracking product warranty details from multiple vendors
- (B) Increased product assembly time due to varied vendor delivery timelines
- (C) **Potential for introduction of insecure or compromised components**
- (D) The need for multiple purchase orders, leading to increased paperwork

Explanation 157. Correct Answer: C. Potential for introduction of insecure or compromised components. When components are sourced from multiple vendors, there is a heightened risk that one or more components might have vulnerabilities or could be compromised, thus impacting the security of the overall product.

The integrity and security of components are vital in product development, especially when those components are part of the supply chain from various vendors. If one vendor has lax security measures or gets compromised, the components they supply can introduce vulnerabilities into the finished product,

affecting its overall security posture and potentially leading to data breaches or other cyber threats.

Option A is incorrect. While tracking warranties is an operational concern, it doesn't pose a direct security risk when sourcing components from multiple vendors.

Option B is incorrect. Product assembly time and vendor delivery timelines are logistical and operational concerns, not primary security risks associated with supply chain vendors.

Option D is incorrect. Managing multiple purchase orders is a business process challenge, not a primary security concern.

Question 158. John, a security analyst, noticed an increase in unauthorized devices connecting to the company's wireless network. To identify the reason, he realized that the wireless access points were still using an old encryption standard. Which outdated encryption standard is likely in use that is known to be easily compromised?

- (A) WPA3
- (B) **WEP**
- (C) WPA2-PSK
- (D) AES

Explanation 158. Correct Answer: B. WEP. Wired Equivalent Privacy (WEP) is an old and outdated encryption protocol for wireless networks. It has several known vulnerabilities and is considered insecure, making it easier for attackers to compromise.

Option A is incorrect. WPA3 is a newer and more secure encryption protocol for wireless networks and is considered a significant improvement over previous standards.

Option C is incorrect. WPA2-PSK (Wi-Fi Protected Access 2 with Pre-Shared Key) is more secure than WEP. While it can still be targeted, it is not as easily compromised as WEP.

Option D is incorrect. AES (Advanced Encryption Standard) is an encryption standard and not a wireless encryption protocol. It is often used within WPA2 and WPA3 for securing wireless data.

Question 159. After being fired from his position as a senior network administrator at XYZ Corp, John discovered a backdoor into the company's main server that he had previously set up. He then initiated a series of Distributed Denial of Service (DDoS) attacks over a month. What is the most probable motivation behind John's actions?

- (A) Ethical concerns about the company's data handling
- (B) Financial gain by selling access to the backdoor
- (C) Desire to research and find vulnerabilities for personal growth
- (D) **Revenge against the company for his termination**

Explanation 159. Correct Answer: D. Revenge against the company for his termination. Given that John acted after being fired and initiated disruptive attacks, it's evident that his actions were motivated by a desire for revenge against his former employer.

Option A is incorrect. There's no indication in the scenario that John had ethical concerns regarding the company's data practices.

Option B is incorrect. The scenario doesn't mention John selling access to the backdoor, only that he initiated DDoS attacks.

Option C is incorrect. John's actions after termination seem malicious rather than a pursuit of knowledge or research.

Question 160. TechBank has just opened a new branch in the city center. Due to its location, the management is concerned about potential vehicular attacks on the facility. Which of the following physical security measures can TechBank employ to specifically deter such attacks?

- (A) Surveillance Cameras
- (B) **Bollards**
- (C) Access Badges
- (D) Security Guards

Explanation 160. Correct Answer: B. Bollards. Bollards are short, sturdy vertical posts that are typically used to control road traffic. In the context of physical security, they serve to prevent vehicles from entering areas where they are not allowed, thereby acting as a deterrent against potential vehicular attacks.

Option A is incorrect. While surveillance cameras can monitor and record activities, they do not serve as a physical barrier against vehicular attacks.

Option C is incorrect. Access badges control personnel access to facilities but do not deter vehicular attacks.

Option D is incorrect. While security guards can respond to threats and control access, they are not a specific measure to deter vehicular attacks like bollards.

Question 161. A financial organization’s high-security data center has an authentication system for its main entry. If the system encounters an unexpected error, the organization wants to ensure that no one can gain access to the data center until the system is fixed. Which configuration should the authentication system be set to?

- (A) Fail-open
- (B) **Fail-closed**
- (C) Fail-secure
- (D) Fail-passive

Explanation 161. Correct Answer: B. Fail-closed. Fail-closed, also known as fail-secure, is a mode where if a system fails, it denies all requests by default, effectively “closing” access. In high-security environments, it’s often preferred to prevent any unauthorized access during system failures.

Option A is incorrect. Fail-open is the opposite of what the organization wants. In a fail-open scenario, if the system fails, it would allow all requests by default.

Option C is incorrect. While “fail-secure” is another term for “fail-closed”, the use of both terms in the options can confuse

the test-taker. In this context, option B is the more appropriate choice.

Option D is incorrect. Fail-passive isn't a standard term in the context of authentication failure modes. Fail-open and fail-closed (or fail-secure) are the primary recognized terms.

Question 162. CyberSecure Inc. is evaluating the financial impact of a potential security breach on its main server. The company has estimated that a breach of this server would lead to a direct financial loss of \$500,000 due to data recovery, legal fees, and fines. Which of the following best represents this estimation?

- (A) Annual Rate of Occurrence (ARO)
- (B) Total Cost of Ownership (TCO)
- (C) **Single Loss Expectancy (SLE)**
- (D) Annualized Loss Expectancy (ALE)

Explanation 162. Correct Answer: C. Single Loss Expectancy (SLE). The Single Loss Expectancy (SLE) represents the expected monetary loss every time a risk occurs. In this case, the company is estimating the direct financial loss from a single breach event.

Option A is incorrect. The Annual Rate of Occurrence (ARO) represents how often the event is expected to occur in a year, not the cost of a single event.

Option B is incorrect. Total Cost of Ownership (TCO) refers to the complete cost of owning a particular asset or solution over its lifecycle, not the cost of a single event.

Option D is incorrect. The Annualized Loss Expectancy (ALE) is a calculated value that represents the expected annual loss, based on the SLE and the ARO.

Question 163. A large e-commerce company wants to ensure that their newly developed application is free from any code vulnerabilities before it is deployed to the production environment. They want to catch any software flaws, especially those that might lead to potential security risks. Which of the following methodologies should they employ?

- (A) Runtime application self-protection (RASP)
- (B) Penetration testing on the live application
- (C) **Static code analysis**
- (D) User acceptance testing (UAT)

Explanation 163. Correct Answer: C. Static code analysis.

Static code analysis involves analyzing the application's code without executing it, focusing on detecting vulnerabilities, coding flaws, or other potential security threats, making it an appropriate methodology for the scenario presented.

Option A is incorrect. Runtime application self-protection (RASP) is about real-time application monitoring and protection, which would not be the primary choice for pre-deployment vulnerability checks.

Option B is incorrect. Penetration testing on the live application involves testing the application once it is live or running, which might not be suitable when looking to identify vulnerabilities in the pre-deployment phase.

Option D is incorrect. User acceptance testing (UAT) focuses on determining if the software meets the business needs and functions correctly for the end-users. It does not emphasize finding security vulnerabilities.

Question 164. In the new branch of BankSecure, the management has decided to install a security system at the main entrance that forces visitors to go through two separate authorization checks before entering the main premises. Which physical security measure should they consider?

- (A) Turnstiles
- (B) Security Guards
- (C) **Access Control Vestibule**
- (D) Keycard Readers

Explanation 164. Correct Answer: C. Access Control

Vestibule. An access control vestibule, often referred to as a mantrap, is a two-stage authentication system. It consists of two doors: a person enters the first door, undergoes an authorization check (like a badge reader or biometric scanner), and only after being approved can they proceed to the second door, where they undergo another authorization check before accessing the main premises.

Option A is incorrect. Turnstiles control the flow of individuals into a location and can prevent tailgating to some extent, but they do not force a two-stage authorization check.

Option B is incorrect. While security guards can perform authorization checks and control access, they alone do not

provide a two-stage authorization system like an access control vestibule.

Option D is incorrect. Keycard readers are a form of access control that checks the credentials of individuals, but on their own, they don't ensure two separate authorization checks.

Question 165. XYZ Corporation recently implemented a security solution that constantly evaluates the company's threat landscape, monitoring for emerging risks and immediately alerting the security team of any changes. This assessment model allows the team to rapidly adapt their security posture in response to live threats. What type of risk assessment is XYZ Corporation utilizing?

- (A) One-time
- (B) Periodic
- (C) Dynamic
- (D) **Continuous**

Explanation 165. Correct Answer: D. Continuous.

Continuous risk assessments involve ongoing and real-time monitoring of risks, enabling an organization to instantly react to emerging threats and vulnerabilities.

Option A is incorrect. A one-time risk assessment is specific to a single event or purpose and is not intended to be repeated regularly.

Option B is incorrect. Periodic risk assessments are carried out at scheduled intervals, such as annually or biannually, and are not ongoing.

Option C is incorrect. Dynamic assessments can adapt to changing environments or factors, but “dynamic” doesn’t specifically denote ongoing, real-time assessment like “continuous” does.

Question 166. A software development company is evaluating the risks associated with a newly discovered vulnerability in its application. After reviewing logs and simulating potential attacks, the security team estimates that there is a 0.25 probability of the vulnerability being exploited in the next year. What does this probability indicate?

- (A) **The vulnerability has a 1 in 4 chance of being exploited in the next year**
- (B) The vulnerability will certainly be exploited four times in the next year
- (C) The vulnerability has been exploited 25 times in the past year
- (D) Every fourth customer will exploit the vulnerability.

Explanation 166. Correct Answer: A. The vulnerability has a 1 in 4 chance of being exploited in the next year. A probability of 0.25 indicates a 25% chance, or a 1 in 4 likelihood, of an event occurring.

Option B is incorrect. A probability value doesn’t predict a definite number of occurrences, just the likelihood of an occurrence.

Option C is incorrect. The probability figure given is an estimate of future risk, not a tally of past events.

Option D is incorrect. The probability provided is not about customers but about the chance of the vulnerability being exploited.

Question 167. During a routine scan, the security team at a graphic design firm discovers that an employee downloaded an image from an email and subsequently, unusual network traffic was detected originating from that employee's workstation. The image appeared normal when opened. What type of attack might have been used in this situation?

- (A) **Image Steganography Malware**
- (B) Password Brute Force
- (C) Phishing
- (D) Port Scanning

Explanation 167. Correct Answer: A. Image Steganography Malware. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. Image steganography specifically involves hiding malicious code within an image. When the image is downloaded or opened, the malicious code can be executed without the victim's knowledge.

Option B is incorrect. Password Brute Force is an attack method where an attacker attempts to guess a user's password by systematically trying every possible combination of letters, numbers, and symbols until the correct password is discovered.

Option C is incorrect. Phishing typically involves deceptive emails or messages attempting to trick recipients into divulging sensitive information. While images can be used in phishing

attempts, the scenario described does not indicate an attempt to extract information from the employee.

Option D is incorrect. Port Scanning is an attempt to discover open ports on a computer, which can reveal services running on those ports. It does not involve the use of images.

Question 168. TechSoft Corp. is implementing a new asset-tracking system to monitor its vast array of computing resources. Which of the following should be the PRIMARY reason for maintaining an up-to-date hardware and software inventory?

- (A) To ensure software licenses are renewed on time
- (B) To identify and respond to unauthorized devices or software promptly**
- (C) To aid in the procurement of new hardware and software
- (D) To provide employees with an understanding of available resources

Explanation 168. Correct Answer: B. To identify and respond to unauthorized devices or software promptly.

While all the options have valid reasons for maintaining an inventory, from a security standpoint, identifying unauthorized devices or software promptly is crucial. Unauthorized devices or software can pose a significant security risk, including potential data breaches or malware infections.

Option A is incorrect. While renewing software licenses is important, it's not the primary security reason for maintaining an inventory.

Option C is incorrect. Procurement decisions benefit from inventory data but do not directly impact immediate security concerns in the way that identifying unauthorized assets does.

Option D is incorrect. While providing employees with resource understanding is beneficial, it isn't as crucial for security as promptly identifying unauthorized assets.

Question 169. Acme Corp, a large organization, has recently entered into a contract with Zenith MSP for IT management and support. The CISO of Acme Corp is concerned about the security risks associated with this new relationship. Which of the following is the PRIMARY security concern when utilizing managed service providers (MSPs) in a supply chain?

- (A) Increased costs due to the integration of new technologies
- (B) Difficulty in ensuring consistent patch management
- (C) **Potential for unauthorized access to company resources**
- (D) Decreased IT staff morale due to outsourcing

Explanation 169. Correct Answer: C. Potential for unauthorized access to company resources. Managed Service Providers usually have elevated privileges to provide their services, potentially making them a prime target for attackers. A breach at the MSP level can lead to unauthorized access to their client's resources.

When a company engages with an MSP, that provider typically has access to critical systems, data, and network infrastructure to deliver their services. If the MSP is compromised, this can

lead to a cascading effect where client systems and data are also vulnerable. It is imperative for companies to ensure their MSPs have robust security postures to prevent unauthorized access.

Option A is incorrect. While cost considerations are important in business decisions, they are not a direct security risk posed by MSPs in a supply chain.

Option B is incorrect. Though ensuring consistent patch management is a legitimate concern, the primary risk is unauthorized access through the MSP, which might have extensive privileges.

Option D is incorrect. While IT staff morale is a valid organizational concern when outsourcing, it is not the primary security risk associated with MSPs.

Question 170. Mike, an employee at a tech company, receives an instant message from a coworker named Jessica. The message contains a link and claims to showcase a hilarious video. However, Mike knows Jessica is on vacation. He suspects the message might not genuinely be from her. What type of threat is Mike most likely encountering?

- (A) Watering Hole Attack
- (B) Man-in-the-Middle Attack
- (C) **IM Spoofing**
- (D) Side-channel Attack

Explanation 170. Correct Answer: C. IM Spoofing. IM Spoofing occurs when an attacker sends messages to a system that appear to come from a trusted source, typically a known

contact. By pretending to be someone the victim knows, the attacker can deceive the victim into opening a malicious link or sharing confidential information.

Option A is incorrect. A Watering Hole Attack is where the attacker guesses or observes which websites the group often uses and infects one or more of them with malware.

Option B is incorrect. A Man-in-the-Middle Attack involves the attacker secretly intercepting and relaying communication between two parties. The attacker makes independent connections with the victims and relays messages between them.

Option D is incorrect. A Side-channel Attack is based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself.

Question 171. At a newly established museum, management wants to install sensors in the exhibit rooms to detect any unauthorized movement after hours. The rooms are often filled with a mix of air conditioning and external noise from the city. Which sensor would be BEST suited to detect movement in such conditions without being affected by the noise?

- (A) Acoustic sensors
- (B) Glass break detectors
- (C) **Ultrasonic sensors**
- (D) Thermal imaging cameras

Explanation 171. Correct Answer: C. Ultrasonic sensors.

Ultrasonic sensors emit high-frequency sound waves to detect motion. These sound waves are beyond the range of human hearing and won't be affected by ambient noise, making them ideal for environments with varying noise conditions. When motion is detected, as indicated by changes in the reflected waves, an alarm is triggered.

Option A is incorrect. Acoustic sensors detect specific sounds. The external noise from the city might cause false alarms or interfere with their detection capabilities.

Option B is incorrect. Glass break detectors are designed to detect the sound or vibration of breaking glass. They aren't designed primarily to detect movement.

Option D is incorrect. Thermal imaging cameras detect heat signatures and would be more susceptible to variations in room temperature due to air conditioning, potentially leading to false detections.

Question 172. A global e-commerce company maintains a risk register to keep track of identified risks and to monitor specific metrics that might indicate an increased risk level. Recently, there has been a 20% increase in abandoned shopping carts on their platform. How should this metric be categorized in the context of the risk register?

- (A) Risk Appetite
- (B) Risk Mitigation Strategy
- (C) **Key Risk Indicator (KRI)**
- (D) Risk Tolerance Threshold

Explanation 172. Correct Answer: C. Key Risk Indicator (KRI). Key Risk Indicators (KRIs) are metrics used to measure and provide an early signal of increasing risk exposures in various areas of an organization. In this scenario, the 20% increase in abandoned shopping carts can serve as a KRI, signaling potential issues like site performance, security concerns, or user experience that may need to be addressed.

Option A is incorrect. Risk appetite refers to the amount of risk an organization is willing to accept in pursuit of its objectives. The increase in abandoned carts doesn't measure this.

Option B is incorrect. A risk mitigation strategy describes actions an organization plans to take to address risks. The metric provided is a measure, not an action or strategy.

Option D is incorrect. Risk tolerance threshold indicates the amount of risk an organization is willing to tolerate. The scenario describes a metric that might indicate an issue, not a predefined threshold.

Question 173. An IT security analyst at a multinational corporation receives an email from the “HR Department” requesting urgent verification of his personal details, including his home address and social security number. The email has the company’s logo but has several spelling errors. Which type of email-based threat is this email most likely representing?

- (A) Business Email Compromise (BEC)
- (B) Email bombing
- (C) Email forwarding
- (D) **Phishing**

Explanation 173. Correct Answer: D. Phishing. Phishing emails aim to deceive recipients into sharing personal or sensitive data by impersonating a trusted source. The email's dubious quality, such as spelling errors, combined with the request for personal details, is indicative of a typical phishing attempt.

Option A is incorrect. While BEC is a type of targeted scam using email, it usually involves impersonating executives or high-ranking officials within an organization to initiate unauthorized fund transfers. The described scenario does not align with that.

Option B is incorrect. Email bombing involves sending large volumes of emails to a single recipient, typically to overwhelm the system or hide other malicious activities. This scenario does not describe such an attack.

Option C is incorrect. Email forwarding refers to the automated redirection of email from one address to another. It is not a direct threat in itself but can be misused. The described scenario does not align with that.

Question 174. TechSoft Corp, a mid-sized software development firm, is relocating its main office to a new building. The management is concerned about potential threats after hours, particularly due to the increasing reports of cyber-espionage. They are evaluating different security measures. Which option would provide an immediate physical presence and deterrence during non-business hours?

(A) CCTV with motion detection

- (B) Retinal scan at all entrances
- (C) **Security guard presence**
- (D) Reinforced doors and windows

Explanation 174. Correct Answer: C. Security guard presence. A security guard provides a visible deterrent and immediate physical presence. This human element is invaluable in situations where an immediate response to threats, deterrence of potential intruders, or evaluation of suspicious activities is required, especially during non-business hours.

Option A is incorrect. While CCTV with motion detection can monitor and alert on movement, it doesn't provide the immediate human response and deterrence a security guard does.

Option B is incorrect. A retinal scan is an authentication mechanism for controlling access. While it offers high security, it doesn't offer the visible deterrence or immediate response of a security guard.

Option D is incorrect. Reinforced doors and windows enhance the physical security of a building, but they don't provide an active and visible human deterrence like a security guard.

Question 175. A multinational corporation has data centers located in different countries. Due to regulatory constraints, remote access to these data centers is highly restricted. The company's IT administrators need a centralized way to access all data centers securely without directly accessing them from their workstations. Which solution should the company

consider?

- (A) Setting up a DMZ
- (B) **Implementing a Jump server**
- (C) Deploying an Active Directory
- (D) Using a local Proxy

Explanation 176. Correct Answer: B. Implementing a Jump server. A Jump server, also known as a bastion host, acts as an intermediary server allowing users to connect to it before accessing another server or network. It provides a controlled means of access between two networks, such as an internal network and an external network.

Option A is incorrect. A DMZ (Demilitarized Zone) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually the internet. It doesn't provide a consolidated access point like a Jump server.

Option C is incorrect. Active Directory is a directory service for Windows domain networks. It's not designed to provide controlled remote access to multiple data centers.

Option D is incorrect. A local Proxy might be used to control internet access or cache web content but doesn't act as a centralized access point for data centers like a Jump server.

Question 176. GammaTech is in the final stages of deploying a new application. Before the deployment, the security team wants to examine the application's code without executing it to identify any potential vulnerabilities. Which vulnerability

identification method should the team employ?

- (A) Penetration Testing
- (B) Dynamic Analysis
- (C) **Static Analysis**
- (D) Fuzz Testing

Explanation 176. Correct Answer: C. Static Analysis. Static analysis involves examining an application's code, bytecode, or binary code without executing it to identify vulnerabilities. This method allows security teams to find potential security issues in the codebase before the application runs.

Option A is incorrect. Penetration testing involves actively trying to exploit vulnerabilities in a system or application. It does not focus on code examination without execution.

Option B is incorrect. Dynamic analysis examines an application during its runtime, observing its behavior to identify vulnerabilities.

Option D is incorrect. Fuzz testing, or fuzzing, involves providing a program with a series of random inputs to see if any of them cause crashes or other unexpected behavior, helping identify vulnerabilities.

Question 177. A cloud-based SaaS company wants to ensure its infrastructure can handle a potential influx of a large number of users in the future. Which of the following approaches would BEST meet this scalability consideration?

- (A) **Implement a horizontal scaling strategy**
- (B) Introduce multi-factor authentication

- (C) Deploy deep packet inspection tools
- (D) Implement a centralized logging system

Explanation 177. Correct Answer: A. Implement a horizontal scaling strategy. Horizontal scaling involves adding more machines or nodes to a system to handle increased load, which can be especially effective in a cloud environment. It allows the infrastructure to accommodate more users by distributing the load among multiple servers.

Option B is incorrect. Multi-factor authentication is essential for security, but it does not address the scalability of the infrastructure to handle a large number of users.

Option C is incorrect. Deep packet inspection tools are used for analyzing network traffic for security and management purposes, but they don't directly enhance the scalability of an infrastructure.

Option D is incorrect. Centralized logging systems help consolidate and analyze logs from various sources, but they do not address the scalability needs of the infrastructure itself.

Question 178. WebServ Corp., a web hosting company, has been analyzing the reliability of its servers. They found that one of their server models, on average, tends to fail once every 2000 hours and then gets promptly repaired. Which of the following metrics is WebServ Corp. evaluating?

- (A) Recovery Time Objective (RTO)
- (B) Mean Time To Repair (MTTR)

- (C) **Mean Time Between Failures (MTBF)**
- (D) Recovery Point Objective (RPO)

Explanation 178. Correct Answer: C. Mean Time Between Failures (MTBF). MTBF (Mean Time Between Failures) is a measure of how reliable hardware or a system is. It's the average time that passes from one failure to the next. For WebServ Corp., the 2000-hour duration between failures reflects the MTBF.

Option A is incorrect. Recovery Time Objective (RTO) is the targeted time and service level within which a business process must be restored after an interruption to avoid unacceptable losses.

Option B is incorrect. Mean Time To Repair (MTTR) represents the average time needed to fix a failed component.

Option D is incorrect. Recovery Point Objective (RPO) measures the amount of data that can be lost, in terms of time, without causing harm to the business continuity.

Question 179. Sarah, an end-user, downloads a software update from a website. Before installing, she wants to make sure the software hasn't been modified maliciously and that it originates from a trusted source. What should Sarah check to validate this?

- (A) The SSL certificate of the website
- (B) **The application's code signing certificate**
- (C) The application's open-source repositories
- (D) The software's user reviews

Explanation 179. Correct Answer: B. The application's code signing certificate. By checking the application's code signing certificate, Sarah can validate that the software was indeed issued by a trusted entity and hasn't been altered since it was signed. A valid code signing certificate gives users confidence in the authenticity and integrity of the software.

Option A is incorrect. While the SSL certificate of a website ensures secure data transmission between the server and the browser, it doesn't guarantee the integrity or authenticity of the software being downloaded.

Option C is incorrect. Open-source repositories may contain the source code of a software, but checking these repositories doesn't necessarily validate the integrity of the compiled software version Sarah has downloaded.

Option D is incorrect. User reviews can provide insights into the software's functionality and user experience, but they cannot be relied upon to confirm software authenticity or integrity.

Question 180. An organization is conducting a risk assessment for its cloud infrastructure. The assessment has determined that the likelihood of a data breach through an insecure API is "High." What factors may have contributed to this likelihood rating?

- (A) The API has been thoroughly tested and has a known secure configuration
- (B) There are few records of this kind of breach in the industry
- (C) The API is publicly accessible and has had several

vulnerabilities reported in the past six months

(D) The cloud provider offers a guaranteed SLA against any form of security breach

Explanation 180. Correct Answer: C. The API is publicly accessible and has had several vulnerabilities reported in the past six months. A publicly accessible API with a history of recent vulnerabilities significantly increases the likelihood of a breach, making this scenario the best fit for a “High” likelihood rating.

Option A is incorrect. A thoroughly tested and known secure configuration would likely reduce the likelihood rating.

Option B is incorrect. Few records of similar breaches would also likely reduce the assessed likelihood.

Option D is incorrect. A guaranteed SLA might offer remedies post-breach, but it does not inherently reduce the likelihood of a breach occurring.

Question 181. Jenny, the new CIO of a multinational firm, wants to ensure that every software and hardware asset in the organization has a clearly defined owner responsible for its security and maintenance. Which of the following is the MOST effective way to achieve this?

(A) Deploy an automated asset discovery tool and assign assets to departments based on their location

(B) Mandate that every department head is the default owner of all assets within their department

(C) Conduct regular audits and require individual users to

claim ownership of their assets

(D) Introduce an Asset Management System where assets are logged with defined ownership as they are procured or assigned

Explanation 181. Correct Answer: D. Introduce an Asset Management System where assets are logged with defined ownership as they are procured or assigned. An Asset Management System provides a structured way to log, track, and manage assets throughout their lifecycle, including defining and recording asset ownership. This ensures clarity and accountability regarding asset responsibility.

Option A is incorrect. While automated discovery tools are helpful, assigning assets based solely on location does not necessarily reflect the actual usage or responsibility for the asset.

Option B is incorrect. While department heads should be aware of assets within their departments, they may not always be the best individuals to take ownership, especially for specific or specialized assets.

Option C is incorrect. Regular audits are crucial, but relying solely on users to claim ownership might not capture all assets, and it's a reactive rather than proactive approach.

Question 182. An organization is deploying new IoT devices in its smart office. To ensure that only authorized devices can connect to the corporate network, each device will be given a unique key pair. Which of the following best describes the

system authentication approach the organization is using?

- (A) Shared secret authentication
- (B) **Public key infrastructure (PKI)**
- (C) Token-based authentication
- (D) Username and password authentication

Explanation 182. Correct Answer: B. Public key infrastructure (PKI). Public key infrastructure (PKI) is a combination of hardware, software, policies, and standards that work together to provide a framework for secure communications. One of the primary features of PKI is the use of a pair of keys (public and private) to authenticate entities. In the scenario, each IoT device is given a unique key pair, indicating the use of PKI for system authentication.

Option A is incorrect. Shared secret authentication typically involves two parties having a shared secret that they use to authenticate one another. The scenario mentions a unique key pair for each device, which doesn't align with the concept of a shared secret.

Option C is incorrect. Token-based authentication typically involves using a hardware or software token that generates a time-sensitive code. The scenario is describing the use of key pairs, not tokens.

Option D is incorrect. Username and password authentication is a method where entities provide a username and a secret password to verify their identity. The scenario does not mention the use of usernames or passwords.

Question 183. After a recent security breach, CyberCorp is reviewing its software vendors for their responsiveness to vulnerabilities. Which of the following metrics would BEST assist CyberCorp in determining the timeliness and efficiency of security patches from a vendor?

- (A) The frequency of software updates released by the vendor
- (B) The vendor's quarterly financial reports
- (C) **Time between vulnerability disclosure and patch release by the vendor**
- (D) The number of features added by the vendor in the last software update

Explanation 183. Correct Answer: C. Time between vulnerability disclosure and patch release by the vendor. The time taken by a vendor to release a security patch after a vulnerability is disclosed is a direct measure of their responsiveness to security threats. A shorter duration indicates a higher prioritization of security concerns.

Option A is incorrect. Frequency of software updates does not necessarily correlate with timely security patches. A vendor might release frequent updates but still be slow in addressing security issues.

Option B is incorrect. A vendor's quarterly financial reports might indicate the financial health of the company but does not directly reflect their responsiveness to security vulnerabilities.

Option D is incorrect. The number of features added in a software update does not indicate the timeliness or effectiveness of security patches.

Question 184. A company is setting up a secure communication channel between its headquarters and a remote branch office. To ensure that data transmitted over this channel originates from a legitimate system at the branch office, the company is considering using digital certificates. Which authentication method for systems is the company contemplating?

- (A) Kerberos authentication
- (B) Password-based authentication
- (C) **Certificate-based authentication**
- (D) Biometric-based authentication

Explanation 184. Correct Answer: C. Certificate-based authentication. Certificate-based authentication uses digital certificates to verify the identity of systems or individuals. In the given scenario, the company wants to verify that data transmitted over the communication channel originates from a legitimate system, making digital certificates an appropriate choice.

Option A is incorrect. Kerberos authentication is a ticket-based authentication protocol primarily used to authenticate users in a network, not specifically for system-to-system authentication using digital certificates.

Option B is incorrect. Password-based authentication requires systems or users to provide a secret password to prove their identity. It doesn't involve the use of digital certificates.

Option D is incorrect. Biometric-based authentication involves using unique physical or behavioral attributes of a person for verification, such as fingerprints or facial patterns. It is not applicable to system-to-system authentication.

Question 185. After a series of cyber incidents, AlphaTech Corp. wants to take proactive measures to identify vulnerabilities in their network. They aim to obtain a comprehensive report of potential weaknesses without exploiting them. Which of the following would best meet this objective?

- (A) Penetration test
- (B) **Vulnerability scan**
- (C) Red team assessment
- (D) Port security

Explanation 185. Correct Answer: B. Vulnerability scan. A vulnerability scan is designed to inspect systems, networks, and applications to identify potential weaknesses or vulnerabilities. Unlike some of the other options, it doesn't attempt to exploit these vulnerabilities; it merely identifies and reports them.

Option A is incorrect. A penetration test goes a step further than a vulnerability scan. While it identifies vulnerabilities, it also attempts to exploit them to understand the potential impact of a breach.

Option C is incorrect. A red team assessment is a goal-based assessment where a simulated adversary (the red team) tries to achieve specific objectives. It often involves exploitation, which goes beyond the mere identification of vulnerabilities.

Option D is incorrect. Port security is a feature at the data link layer to control MAC address-based access on a port-by-port basis. It doesn't offer a comprehensive vulnerability report.

Question 186. Lucy, a security analyst, is informed that several employees have been receiving unauthorized file transfer requests via Bluetooth when they are in the company's cafeteria. Which of the following attacks is MOST likely being attempted?

- (A) **Bluejacking**
- (B) ARP poisoning
- (C) Bluesnarfing
- (D) Evil Twin

Explanation 186. Correct Answer: A. Bluejacking.

Bluejacking is the sending of unsolicited messages or files over Bluetooth to Bluetooth-enabled devices such as mobile phones, laptops, or PDAs. It is often used as a prank or to advertise to nearby people.

Bluejacking does not give attackers control over the victim's device, but it can be used to send unwanted messages or files, which aligns with the scenario described.

Option B is incorrect. ARP poisoning is a type of attack in which an attacker sends falsified ARP (Address Resolution Protocol) messages over a local area network. It's unrelated to Bluetooth communications.

Option C is incorrect. Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth

connection. Bluesnarfing goes beyond just sending unsolicited messages; it seeks to access personal data.

Option D is incorrect. An Evil Twin attack involves creating a rogue Wi-Fi hotspot to masquerade as a legitimate one, to intercept or manipulate data traffic. It does not directly involve Bluetooth connections.

Question 187. A small business wants to deploy a single network security device that can handle multiple security functions such as firewall protection, intrusion detection, anti-malware, and content filtering. Which of the following would be the most suitable solution?

- (A) Network Intrusion Detection System (NIDS)
- (B) Web Application Firewall (WAF)
- (C) **Unified Threat Management (UTM)**
- (D) Proxy Server

Explanation 187. Correct Answer: C. Unified Threat Management (UTM). Unified Threat Management (UTM) devices are designed to combine multiple security features into a single appliance. This makes them ideal for smaller organizations that require a comprehensive range of security functions but might not have the resources to deploy and manage multiple standalone devices.

Option A is incorrect. While NIDS can identify and notify of potential malicious activities, it does not offer the comprehensive multi-feature capabilities found in a UTM.

Option B is incorrect. A Web Application Firewall (WAF) specifically protects web applications from certain types of attacks like XSS and SQL injection. It does not encompass the broader range of security functions that a UTM does.

Option D is incorrect. A Proxy Server primarily controls internet access and might provide some caching and content filtering capabilities, but it doesn't offer the wide range of security functions that a UTM does.

Question 188. During an audit review at NetSecure Corp., the external auditors observed that the company is willing to take risks that can potentially result in a 10% decrease in their annual profits, but no more than that. The auditors want to document this finding in their report. Which term should they use to describe NetSecure Corp.'s stance?

- (A) Risk Avoidance
- (B) Risk Transfer
- (C) **Risk Tolerance**
- (D) Risk Assessment

Explanation 188. Correct Answer: C. Risk Tolerance. Risk tolerance represents the maximum amount of risk an entity is willing to accept or tolerate. NetSecure Corp.'s acceptance of risks that can result in up to a 10% decrease in annual profits represents their risk tolerance level.

Option A is incorrect. Risk avoidance means completely sidestepping any activities that have associated risks. The scenario indicates that the company is willing to take risks, but within certain limits.

Option B is incorrect. Risk transfer involves offloading certain risks to other parties, typically through insurance or other contractual methods. The scenario doesn't provide information about transferring risks.

Option D is incorrect. Risk assessment is the overall process of identifying, analyzing, and evaluating risks. The scenario is more focused on the company's willingness to accept a specific level of risk rather than assessing it.

Question 189. SecureWeb LLC, a web hosting company, has experienced two server breaches over the past five years. They are currently analyzing the risks associated with their infrastructure. Which of the following best represents the Annualized Rate of Occurrence (ARO) for the server breaches?

- (A) 0.2
- (B) **0.4**
- (C) 2
- (D) 5

Explanation 189. Correct Answer: B. 0.4. The Annualized Rate of Occurrence (ARO) is a measure of how often an event is expected to occur on an annual basis. Given that there have been two breaches over five years, the ARO would be 2 breaches divided by 5 years, which is 0.4.

Option A is incorrect. While it's close, the calculation for ARO should be the number of occurrences (2) divided by the number of years (5), which is 0.4, not 0.2.

Option C is incorrect. This would indicate two breaches every year, which is not the case presented.

Option D is incorrect. This would suggest that the breaches happen five times a year, which is inconsistent with the scenario.

Question 190. DataCenter Inc. is located in a region prone to protests and vandalism. They wish to enhance their perimeter security to deter potential intruders and make it visibly clear that unauthorized access is restricted. Which of the following physical security measures would be the most effective first line of defense for the company?

- (A) Sliding Doors
- (B) Security Cameras
- (C) **High-security Fencing**
- (D) Proximity Card Readers

Explanation 190. Correct Answer: C. High-security Fencing.

High-security fencing is a primary physical barrier that serves to deter, delay, and detect intrusions. It provides a clear visual indicator that delineates private property and can be equipped with additional deterrents such as barbed wire or sensors.

Especially in areas prone to vandalism or protests, a robust fence acts as an immediate barrier to unauthorized access.

Option A is incorrect. Sliding doors are more applicable to internal security or entrance points and do not serve as a primary external barrier.

Option B is incorrect. While security cameras monitor and record activities, they do not serve as a physical barrier to prevent or deter unauthorized access.

Option D is incorrect. Proximity card readers are a form of access control that checks the credentials of individuals but do not serve as a primary deterrent against vandalism or protests.

Question 191. A financial institution is shutting down one of its data centers. Given the highly sensitive nature of the data stored, the company wants to ensure that there is no possibility of data retrieval from the storage devices. Which of the following methods would be the MOST effective in guaranteeing the destruction of data?

- (A) Overwriting with zeros
- (B) Standard Disk Format
- (C) **Physical Destruction**
- (D) Running a Disk Cleanup utility

Explanation 191. Correct Answer: C. Physical Destruction.

Physical destruction, such as shredding or incinerating the storage devices, ensures complete destruction of the media, making data retrieval impossible, regardless of the tools or techniques employed.

Option A is incorrect. Overwriting with zeros is a method of data sanitization, but advanced techniques might still retrieve some portions of the data.

Option B is incorrect. A standard disk format often does not remove data entirely, and traces can remain that could be recovered with specialized software.

Option D is incorrect. Disk Cleanup utilities are designed to free up space by removing temporary and unnecessary files but not to securely erase sensitive data.

Question 192. Maria, a network administrator, receives a report detailing several open service ports on critical company servers. She wants to verify the accuracy of the report. Which of the following tools would be BEST for Maria to use to validate the findings?

- (A) Password cracker
- (B) **Port scanner**
- (C) IDS (Intrusion Detection System)
- (D) Web application firewall

Explanation 192. Correct Answer: B. Port scanner. A port scanner, such as Nmap, sends packets to specific ports on a network and then listens for responses. This allows the scanner to determine which ports are open and potentially identify the services running on those ports.

Option A is incorrect. Password crackers are used to identify weak or easily guessable passwords. They don't validate open service ports.

Option C is incorrect. An IDS monitors network traffic for suspicious activity. While it can identify potential attacks, it doesn't directly verify open service ports.

Option D is incorrect. A web application firewall (WAF) protects web applications by monitoring, filtering, and blocking potentially harmful HTTP traffic. It doesn't serve the purpose of validating open service ports.

Question 193. Acme Corp is restructuring its internal network to improve its security posture. They aim to separate areas with different levels of trust. Which of the following approaches would BEST achieve this objective?

- (A) Implementing VLANs based on organizational departments
- (B) Setting up a perimeter firewall to segment external and internal traffic
- (C) **Designing network zones based on data sensitivity and access requirements**
- (D) Using a single, flat network for simplicity

Explanation 193. Correct Answer: C. Designing network zones based on data sensitivity and access requirements.

Zoning based on data sensitivity and access requirements ensures that segments of the network with varying trust levels are isolated. This reduces the risk of a breach in one zone affecting another.

Option A is incorrect. While VLANs can segment traffic, doing so based purely on organizational departments may not align with varying trust and data sensitivity requirements.

Option B is incorrect. While perimeter firewalls are crucial for security, they primarily separate internal from external traffic

and don't segment areas of varying trust within the internal network.

Option D is incorrect. A single, flat network doesn't provide segmentation, making it vulnerable to lateral movement if a threat actor gains access.

Question 194. A company has recently upgraded its wireless infrastructure and wants to ensure that the data transmitted over its wireless network is protected using the most recent and secure encryption standards. Which of the following should the company configure on its wireless access points?

- (A) WEP
- (B) WPA
- (C) WPA2
- (D) **WPA3**

Explanation 194. Correct Answer: D. WPA3. WPA3 is the latest iteration of Wi-Fi Protected Access, designed to improve upon the security features of WPA2. It offers enhanced protections against brute-force attacks, superior encryption methods, and a more secure handshake process.

Option A is incorrect. WEP (Wired Equivalent Privacy) is an outdated and insecure protocol that can be easily cracked. It should not be used for securing wireless networks.

Option B is incorrect. While WPA (Wi-Fi Protected Access) was a significant improvement over WEP, it has been surpassed by both WPA2 and WPA3 in terms of security features.

Option C is incorrect. WPA2 has been a strong standard for many years but has vulnerabilities that WPA3 addresses, making WPA3 the more secure option.

Question 195. AlphaTech is conducting a risk analysis on their new online payment gateway. They've calculated the Annual Rate of Occurrence (ARO) for a specific vulnerability as 2, and the Single Loss Expectancy (SLE) as \$50,000. How much should AlphaTech anticipate losing annually due to this vulnerability?

- (A) \$10,000
- (B) **\$100,000**
- (C) \$25,000
- (D) \$1,000,000

Explanation 195. Correct Answer: B. \$100,000. The Annualized Loss Expectancy (ALE) is calculated by multiplying the Annual Rate of Occurrence (ARO) by the Single Loss Expectancy (SLE). In this scenario, $ALE = 2 \times \$50,000 = \$100,000$.

Option A is incorrect. This does not correctly apply the formula for ALE.

Option C is incorrect. This is half of the Single Loss Expectancy and does not represent an annual loss.

Option D is incorrect. This amount is significantly higher than the calculated ALE.

Question 196. After a recent security breach, CyberSolutions Inc. evaluated their response metrics and determined that, on average, it took 4 hours from identifying a security breach to having it completely resolved. Which metric best describes this 4-hour timeframe?

- (A) Recovery Time Objective (RTO)
- (B) Recovery Point Objective (RPO)
- (C) Mean Time Between Failures (MTBF)
- (D) **Mean Time To Repair (MTTR)**

Explanation 196. Correct Answer: D. Mean Time To Repair (MTTR). MTTR (Mean Time To Repair) is a basic measure of the maintainability of repairable items. It represents the average time required to repair a failed component or device. For CyberSolutions Inc., the 4-hour duration from identifying to resolving the breach reflects the MTTR.

Option A is incorrect. Recovery Time Objective (RTO) is the targeted duration of time within which a business process must be restored after a disaster to avoid unacceptable consequences.

Option B is incorrect. Recovery Point Objective (RPO) represents the maximum acceptable amount of data loss measured in time.

Option C is incorrect. Mean Time Between Failures (MTBF) is the predicted elapsed time between inherent failures of a mechanical or electronic system, during normal system operation.

Question 197. A financial application allows users to transfer money to other accounts by entering the account number and the amount to transfer. During a security audit, it was observed that malicious users could enter SQL code into the account number field to manipulate the application's database. Which security technique should the development team implement to address this vulnerability?

- (A) Code obfuscation
- (B) **Input validation**
- (C) Encryption at rest
- (D) Session timeout

Explanation 197. Correct Answer: B. Input validation. Input validation ensures that only valid and expected data is accepted by an application. By validating and sanitizing user input, the application can prevent malicious data, such as SQL code, from being processed and executed, thus mitigating the risk of SQL injection attacks.

Option A is incorrect. Code obfuscation makes it more difficult for attackers to understand the application's code but does not prevent them from injecting malicious input.

Option C is incorrect. Encryption at rest protects stored data, but it doesn't prevent SQL injection attacks which exploit the application's input handling.

Option D is incorrect. Session timeout limits the duration of a user's session, but it does not validate or sanitize user input.

Question 198. GreenTech Inc. is selling a set of old servers to another company. Before the transaction, they want to ensure the data on these servers is irretrievable and they can prove that due diligence was performed. What should GreenTech seek to assure the buyer of proper data destruction?

- (A) A receipt of sale for the servers
- (B) A detailed log of the server's usage
- (C) **A certificate of data sanitization**
- (D) A user manual of the servers

Explanation 198. Correct Answer: C. A certificate of data sanitization. A certificate of data sanitization from a reputable entity provides assurance that all data on the servers was securely and completely wiped. Such certificates confirm that specific techniques were used to ensure data is irretrievable, giving confidence to the buyer.

Option A is incorrect. A receipt of sale only proves the transaction took place but does not address data sanitization or destruction.

Option B is incorrect. A log of the server's usage might detail its operational history but does not provide assurance of data destruction.

Option D is incorrect. A user manual provides instructions on how to use the server but does not address the state or security of the data it once held.

Question 199. A healthcare organization uses a software platform to manage patient records. A recent vulnerability

assessment identified a potential exploit where an unauthorized individual might gain access to 30% of stored patient data.

Which of the following BEST describes this scenario?

- (A) The threat likelihood is 30%
- (B) The vulnerability has a 30% rate of occurrence
- (C) **The exposure factor of the vulnerability is 30%**
- (D) 30% of the patients have been impacted

Explanation 199. Correct Answer: C. The exposure factor of the vulnerability is 30%. The exposure factor is a measure of the magnitude of loss or percentage of asset value that a realized threat would destroy or damage. In this case, the vulnerability could lead to 30% of patient data being accessed.

Option A is incorrect. Likelihood refers to the probability of an event happening, not the potential impact or amount of data that might be exposed.

Option B is incorrect. The rate of occurrence (ARO) is a measure of how often a specific event will occur, not the potential impact or amount of data that might be exposed.

Option D is incorrect. The scenario does not indicate that 30% of patients have already been impacted, only that their data might be accessed if the vulnerability is exploited.

Question 200. GreenTech Industries has a manufacturing facility located in a relatively secluded area. Recent incidents of theft and trespassing have alarmed the management. Which of the following would MOST effectively deter unauthorized nighttime access to the perimeter of the facility?

- (A) Installing infrared sensors
- (B) **Using bright perimeter lighting**
- (C) Deploying additional security guards inside the facility
- (D) Increasing the height of the facility walls

Explanation 200. Correct Answer: B. Using bright perimeter lighting. Bright perimeter lighting acts as a strong deterrent for unauthorized individuals, as it reduces hiding spots, makes surveillance cameras more effective, and can make it easier for security personnel to spot potential threats. In secluded areas, proper lighting is particularly essential to illuminate dark spots and deter potential intruders.

Option A is incorrect. While infrared sensors can detect movement, they do not act as a visible deterrent in the same way bright lighting does.

Option C is incorrect. Deploying additional security guards inside the facility does not address the immediate concern of unauthorized nighttime access to the perimeter.

Option D is incorrect. Increasing the height of the walls can act as a deterrent, but it doesn't illuminate or expose potential intruders like bright lighting does.

EXAM SIMULATOR #3

Questions 201-300

Question 201. An international bank is setting up a new online portal for its customers to access their financial statements. Which measure should the bank implement to ensure that financial data in transit between the customer's browser and the bank's servers is kept confidential?

- (A) Use file-level encryption for all financial statements
- (B) Implement a Web Application Firewall (WAF)
- (C) Use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for the portal
- (D) Store all financial data in an encrypted database

Question 202. A multinational organization with multiple branch offices is looking to simplify their WAN connectivity and reduce costs while ensuring that their inter-office data transfers remain secure. Which technology would best fit their needs?

- (A) VLAN
- (B) MPLS
- (C) SD-WAN
- (D) DMZ

Question 203. While setting up a new internal web application, Laura, a system administrator, decides to use a digital certificate for SSL/TLS encryption. Due to budget constraints, she can't

procure a certificate from a commercial Certificate Authority (CA). Which of the following would be a viable option for Laura to secure the application?

- (A) Rely on plaintext HTTP for the application
- (B) Obtain a certificate from a free Certificate Authority
- (C) Generate a self-signed certificate
- (D) Use a shared certificate from another application

Question 204. A renowned technology company recently released a new line of routers. After a short period, security researchers discovered that some of these routers contain malicious chips embedded during the manufacturing process. This incident most likely represents a vulnerability related to which supply chain aspect?

- (A) Outsourced software development risks
- (B) Service provider's outdated security practices
- (C) Hardware provider's embedded compromise
- (D) Inadequate vendor background checks

Question 205. A multinational corporation is expanding its operations in various countries. The company has decided to restrict access to its internal network based on geolocation to ensure that only employees from specific countries can access certain data. Which of the following would be the MOST appropriate solution to implement this requirement?

- (A) Deploy a VPN with multi-factor authentication
- (B) Use MAC address filtering on all company devices
- (C) Implement a geolocation-based access control system
- (D) Set up region-specific SSIDs for the company's Wi-Fi network

Question 206. TechGuard Inc. and CloudSecure are two cybersecurity firms that are considering a collaboration on a new cloud security project. Both companies have proprietary technologies and methodologies they will bring into the partnership. Before embarking on the collaborative venture, which agreement should they finalize to define the terms of their partnership, roles, and shared responsibilities?

- (A) Non-disclosure agreement (NDA)
- (B) Service-level agreement (SLA)
- (C) Business partners agreement (BPA)
- (D) Memorandum of understanding (MOU)

Question 207. A security team recently upgraded their intrusion detection system (IDS). Since the upgrade, the system hasn't flagged any intrusions, even though intrusion attempts are a regular occurrence. What is this situation best characterized as?

- (A) A true negative
- (B) A false negative
- (C) A true positive
- (D) A confirmation feedback

Question 208. CyberTech Inc., a cybersecurity consulting company, is in discussions with a potential client, MedCorp, to assist in developing a new secure medical records system. MedCorp will be sharing sensitive patient data with CyberTech as part of the process. Which agreement should be in place before the sharing of such information to ensure confidentiality?

- (A) Memorandum of understanding (MOU)
- (B) Service-level agreement (SLA)
- (C) Non-disclosure agreement (NDA)
- (D) Work order (WO)/statement of work (SOW)

Question 209. While analyzing server logs, Mike, an IT security analyst, noticed that an unfamiliar document was frequently accessed. Upon investigation, he realized that this document was deliberately placed by the security team and had no real data but was closely monitored. The purpose of this file is MOST likely:

- (A) To serve as a redundancy copy in case of data loss
- (B) To act as a decoy to attract and detect unauthorized access
- (C) To maintain a record of all user activities for auditing
- (D) To be encrypted and sent to clients as a sample

Question 210. After implementing a major security update to its database system, TechCo experienced unexpected downtime and system incompatibilities. The CISO wants to ensure that such incidents can be quickly addressed in the future. Which of the following should TechCo have had in place before deploying the update to mitigate the impact of these kinds of incidents?

- (A) A comprehensive list of all updates
- (B) An automated system recovery tool
- (C) A backout plan
- (D) A detailed user manual for the update

Question 211. TechFirm is preparing to embark on a new project with a client, focusing on implementing a cybersecurity infrastructure overhaul. They wish to lay out the specific tasks, deliverables, timelines, and resources required for this project. Which type of agreement would best capture these details?

- (A) Memorandum of understanding (MOU)
- (B) Joint venture agreement

- (C) Master service agreement (MSA)
- (D) Work order (WO)/statement of work (SOW)

Question 212. The IT department of a large corporation is performing a vulnerability assessment on its virtualized infrastructure. They come across a potential threat where a user from within a VM can interact and possibly compromise the host system. What is this type of vulnerability commonly referred to as?

- (A) VM cloning
- (B) VM snapshotting
- (C) VM escape
- (D) VM migration

Question 213. A large organization is considering deploying a solution that will allow employees to securely access company resources remotely using their personal devices. The organization wants a solution that can provide strong authentication and ensure that the data remains confidential during transit. Which technology should be adopted?

- (A) Kerberos
- (B) Remote Desktop Services (RDS)
- (C) Remote Access VPN
- (D) SNMP

Question 214. A security analyst at ZetaTech is looking to gather information about emerging threats and vulnerabilities relevant to their industry. Which of the following would be the MOST suitable method to obtain real-time, continuously updated data on potential security issues?

- (A) Relying solely on automated internal vulnerability

scanners

- (B) Periodic manual penetration testing
- (C) Subscribing to an OSINT threat feed
- (D) Regularly checking the company's firewall logs

Question 215. While conducting a security assessment, Lucy found that a specific application crashes when she inputs a string that is much longer than what the input field is designed to handle. This could potentially allow her to execute arbitrary code in the application's context. What vulnerability is Lucy likely trying to exploit?

- (A) SQL Injection
- (B) Cross-Site Scripting (XSS)
- (C) Buffer Overflow
- (D) Directory Traversal

Question 216. WebFirm, a web development company, did not comply with the data handling and protection clauses outlined in their contract with RetailMax, an e-commerce company. As a result, RetailMax's customer data was exposed in a data breach. Which of the following is the MOST probable contractual impact on WebFirm due to this incident?

- (A) WebFirm will receive bonuses for early project completion
- (B) WebFirm will be required to provide additional services at no cost
- (C) RetailMax will terminate the contract and may seek damages
- (D) RetailMax will extend the project timeline

Question 217. During a political campaign, an anonymous group releases a series of articles containing fabricated data about a candidate's past, intending to influence voters' opinions. This is an example of:

- (A) Impersonation
- (B) SSmishing
- (C) Disinformation
- (D) Baiting

Question 218. A multinational company is considering using a cloud storage provider based in a foreign country to store customer data. The company's home country has strict data protection laws that require customer data to remain within its borders. Which of the following considerations is MOST critical for the company when choosing the cloud storage provider?

- (A) The speed of data access from the foreign-based cloud storage
- (B) The encryption standards used by the foreign cloud provider
- (C) Whether the foreign cloud provider offers data storage exclusively within the company's home country
- (D) The reputation and customer reviews of the foreign cloud provider

Question 219. BetaTech, a tech manufacturing firm, wants to ensure that a potential compromise of its IoT devices will not endanger its primary manufacturing control systems. Which of the following approaches would be most effective in achieving this?

- (A) Using a single robust firewall for the entire network

- (B) Periodic password changes for IoT devices
- (C) Segmenting the IoT devices from the manufacturing control systems
- (D) Enabling automatic updates for all IoT devices

Question 220. A software company is developing a new cloud-based application where clients can store and manage their customer contact details. The stored data does not include financial or medical information but does contain phone numbers and email addresses. How should this information be classified?

- (A) Public
- (B) Restricted
- (C) Sensitive
- (D) Classified

Question 221. A multinational company wants to allow its remote employees to securely access the corporate intranet over the Internet. The company's primary concern is to ensure data confidentiality and integrity during transit. Which solution should the company implement?

- (A) VLAN
- (B) VPN
- (C) NAC
- (D) DMZ

Question 222. A financial firm outsources its payment processing to a third-party service provider. After a series of fraudulent transactions, it was discovered that the service provider was not employing the latest encryption standards when transmitting data. Which vulnerability related to supply

chain does this scenario highlight?

- (A) Inadequate vendor background checks
- (B) Service provider's outdated security practices
- (C) Deficient hardware components from a supplier
- (D) Software with embedded backdoors

Question 223. A popular online shopping platform noticed that some product reviews contained a strange link which, when clicked, led users to a site that resembled the platform but harvested login credentials. What vulnerability in the review system might have allowed attackers to post such links?

- (A) Session Hijacking
- (B) Cross-site scripting (XSS)
- (C) Password Spraying
- (D) Credential Stuffing

Question 224. An organization has decided to focus on securing its database servers where customer details and transaction records are stored. This data is not being actively accessed or processed. Which type of security measure would be MOST appropriate for this type of data?

- (A) VLDData Loss Prevention (DLP) for emailAN
- (B) Web Application Firewall (WAF)
- (C) Full Disk Encryption (FDE)
- (D) Intrusion Detection System (IDS) for network traffic

Question 225. XYZ Corp. has recently developed a new manufacturing process that reduces production costs by 50%. This process is not yet patented and is considered a trade secret. The company wants to ensure that employees do not disclose this process to competitors. Which of the following would be

the MOST effective strategy to achieve this?

- (A) Providing employees with a bonus for keeping the process confidential
- (B) Conducting random checks of employee communications
- (C) Implementing a mandatory non-disclosure agreement (NDA) for all employees
- (D) Hosting quarterly seminars to educate employees about the value of the trade secret

Question 226. While analyzing a vulnerability in a company's web application, the security team refers to a specific CVE to understand the vulnerability's details. They further assess its CVSS score to decide on the remediation urgency. Which of the following best describes the purpose of the CVE and CVSS in this context?

- (A) CVE provides a severity score, while CVSS gives a unique identifier for the vulnerability
- (B) CVE and CVSS both offer a scoring mechanism to rank vulnerabilities
- (C) CVE provides a unique identifier, while CVSS offers a standardized severity score
- (D) CVE and CVSS are regulatory requirements for all software applications

Question 227. During a security assessment, Maria, a security consultant, identifies a self-signed certificate being used on a client's public-facing web server. What is the PRIMARY security concern related to this finding?

- (A) The web server might be vulnerable to Distributed Denial of Service (DDoS) attacks

- (B) The certificate could be expired
- (C) Users cannot validate the authenticity of the website easily
- (D) The web server might not support modern encryption algorithms

Question 228. Julia, a security administrator, is concerned about potential unauthorized access to confidential project files stored on a company server. She decides to place a document within the project folders that seems enticing but is actually monitored for access. This strategy aims to detect if someone is accessing files without authorization. What is this document commonly known as?

- (A) Salt file
- (B) Honeyfile
- (C) Log file
- (D) Backup file

Question 229. A security auditor found that a website's login form returns detailed error messages like "Incorrect column name" or "Table not found." Which type of vulnerability could attackers potentially exploit using this information?

- (A) Brute Force Attack
- (B) Structured Query Language injection (SQLi)
- (C) Man-in-the-Middle Attack
- (D) Session Hijacking

Question 230. A law firm is transitioning to a digital storage system and wants to ensure that client records and case files are protected from unauthorized access. Which of the following would be the BEST strategy to ensure the confidentiality of

legal information stored digitally?

- (A) Conducting regular penetration testing on the digital storage system
- (B) Encrypting the client records and case files
- (C) Applying watermarks to digital documents
- (D) Limiting physical access to the server room

Question 231. While conducting a routine security review, Jake, a security specialist, discovers an unexpected piece of data placed in the organization's financial system. Upon asking, he learns that this piece of data is intentionally placed and monitored to see if any unauthorized user or system interacts with it. What is this deceptive piece of data known as?

- (A) Honeysting
- (B) Honeytoken
- (C) Canary token
- (D) Security marker

Question 232. You are a security consultant for a company that uses a cloud-based infrastructure. During a security review, you discover that there are no boundaries defined between the company's development, testing, and production environments in the cloud. This can lead to unintended interactions and data leaks. What kind of vulnerability is this scenario illustrating?

- (A) Insecure API endpoints
- (B) Weak encryption methods
- (C) Lack of resource isolation
- (D) Insufficient backup strategies

Question 233. AlphaCorp is in the final stages of selecting a cybersecurity consultant. One of the shortlisted firms,

SecureWorld, recently hired AlphaCorp's former CISO as a senior consultant. Given this situation, what should be AlphaCorp's immediate concern during vendor selection?

- (A) The expertise the former CISO brings to SecureWorld
- (B) The possibility that SecureWorld could offer a discounted price
- (C) Potential conflict of interest due to prior associations
- (D) SecureWorld's global presence and reputation

Question 234. An IT technician is performing a routine security audit of a company's server room. She discovers a server with outdated firmware that hasn't been updated for two years. What potential vulnerability does the outdated firmware expose the server to?

- (A) SQL Injection
- (B) Physical tampering
- (C) Unpatched exploits
- (D) Credential stuffing

Question 235. As part of the company's vulnerability management initiative, the security team has decided to conduct a series of penetration tests. Which of the following is the PRIMARY reason for incorporating penetration testing as a threat identification method?

- (A) To ensure compliance with regulatory requirements
- (B) To validate the efficiency of security awareness training
- (C) To actively exploit vulnerabilities and assess potential impact
- (D) To identify misconfigurations in the SIEM system

Question 236. Globex Industries is expanding its data centers across multiple geographic locations. The IT team wants to have a centralized system to get real-time status, outages, and metrics of all data center infrastructures. Which of the following solutions would be the MOST effective for this purpose?

- (A) Data Loss Prevention (DLP) tools
- (B) Distributed Denial of Service (DDoS) protection
- (C) Security Information and Event Management (SIEM)
- (D) Infrastructure Management Platform (IMP)

Question 237. After undergoing a major infrastructure upgrade, GlobalMed Corp experienced several unanticipated security issues. In retrospect, the IT manager realized they skipped an essential step in their change management process which could have predicted and mitigated these issues. What step did they most likely overlook?

- (A) Procurement of new hardware
- (B) Training of IT staff on the new systems
- (C) Impact analysis
- (D) Integration with legacy systems

Question 238. Sarah, a software developer at a tech company, decided to gain root access to her company-issued mobile device to customize its features. Soon after, the IT department detected unauthorized data transmissions from her device. Which mobile vulnerability is most likely associated with her actions?

- (A) Side loading of applications
- (B) Inconsistent OS updates
- (C) Mobile device jailbreaking
- (D) Use of open Wi-Fi networks

Question 239. Jenna, a web administrator for a growing online retail business, is in the process of obtaining SSL certificates for the company's domain. The company uses several subdomains for different services, such as shop.example.com, blog.example.com, and support.example.com. Instead of obtaining individual certificates for each subdomain, Jenna wants to use one certificate. What type of certificate should Jenna pursue?

- (A) Extended Validation Certificate
- (B) Wildcard Certificate
- (C) Certificate with Subject Alternative Names (SAN)
- (D) Code Signing Certificate

Question 240. CyberLock Inc. is assessing the security postures of its third-party vendors to determine potential risks. The cybersecurity team wants to gather foundational security information from each vendor to evaluate their security maturity and practices. What would be the most cost-effective and efficient way to collect this data from a large number of vendors?

- (A) Conduct a penetration test for each vendor
- (B) Send out security questionnaires to each vendor
- (C) Visit each vendor's site for an in-person assessment
- (D) Review the annual financial reports of each vendor

Question 241. A developer has implemented a new feature on a company's website that allows users to search for products by their names. Within a few days, the IT team noticed abnormal activities where entire tables from the database were being dumped. Which vulnerability might the new feature have introduced?

- (A) Cross-Site Scripting (XSS)
- (B) Distributed Denial-of-Service (DDoS)
- (C) Structured Query Language injection (SQLi)
- (D) Cross-Site Request Forgery (CSRF)

Question 242. DeltaSoft has released a new web application. The security team is tasked with observing the application's behavior and responses when it is running to identify potential vulnerabilities. Which method is most appropriate for this purpose?

- (A) Static Analysis
- (B) Fuzz Testing
- (C) Whitebox Testing
- (D) Dynamic Analysis

Question 243. GlobalTech, a multinational corporation, is negotiating a cloud storage contract with CloudCorp. GlobalTech wants to ensure that data retrieval times remain under 2 seconds 99.9% of the time. Which component should be explicitly defined in their agreement to set this expectation?

- (A) Pricing model
- (B) Data sovereignty clauses
- (C) Service-level agreement (SLA)
- (D) Termination clauses

Question 244. SoftTech Inc., a software company, is considering expanding its operations to Europe. They will be collecting and processing personal data of EU citizens. Which of the following legal implications is MOST critical for SoftTech Inc. to consider?

- (A) The need to register with each country's software

association

- (B) Compliance with the General Data Protection Regulation (GDPR)
- (C) Ensuring software patent rights in each European country
- (D) The European standard for software coding

Question 245. A multinational organization recently experienced a significant security breach. After investigating, it was determined that a change to the network infrastructure was made without undergoing the standard approval process. As a result, there was a misconfiguration which allowed unauthorized access. What security principle related to change management did the organization neglect?

- (A) Configuration baseline reviews
- (B) Least privilege enforcement
- (C) Approval process adherence
- (D) Patch management

Question 246. Carlos, an IT consultant, advises a startup company on cybersecurity best practices. The company plans to launch several microsites under various subdomains. They want a solution that is cost-effective but also ensures that the sites are validated by a third-party. What type of certificate should Carlos recommend?

- (A) A separate self-signed certificate for each microsite
- (B) An individual third-party certificate for each subdomain
- (C) A third-party wildcard certificate
- (D) An EV certificate issued by an internal CA

Question 247. Two university research departments, UniAlpha and UniBeta, decide to collaborate on a project exploring quantum computing's security implications. They need an agreement to express mutual intentions without enforcing legally binding obligations. Which document is most suitable for their needs?

- (A) Service-level agreement (SLA)
- (B) Non-disclosure agreement (NDA)
- (C) Memorandum of understanding (MOU)
- (D) Licensing agreement

Question 248. A system administrator notices that an unauthorized user was able to obtain elevated privileges on a server, even though the default account settings were configured correctly. Upon investigation, it was found that the server's operating system had not been updated for several months. What type of vulnerability was likely exploited?

- (A) Application Misconfiguration
- (B) OS Patch Management Issue
- (C) Weak Encryption Algorithm
- (D) Password Reuse Attack

Question 249. Jane, an accountant in a multinational corporation, received an email from what seemed to be the company's IT department. The email had the company's logo, colors, and font and urged Jane to click on a link to reset her password due to "suspicious activity." However, upon close inspection, Jane noticed a minor spelling error in the domain name of the sender's email address. What type of attack does this scenario describe?

- (A) Spear Phishing

- (B) Vishing
- (C) Baiting
- (D) Brand Impersonation

Question 250. As the Chief Security Officer (CSO) of AlphaTech, you are in the process of finalizing a partnership agreement with a third-party provider. To ensure ongoing security compliance and transparency, you want to reserve the right for your organization to inspect the vendor's operations and security measures in the future. Which clause should you ensure is included in the contract?

- (A) Non-disclosure agreement (NDA)
- (B) Service level agreement (SLA)
- (C) Termination clause
- (D) Right-to-audit clause

Question 251. After a major security incident, DeltaTech implemented several security patches to address vulnerabilities in their infrastructure. To ensure the effectiveness of these patches, what should be DeltaTech's primary next step?

- (A) Deploy additional firewalls at the network perimeter
- (B) Provide cybersecurity training to all employees
- (C) Rescan the systems to check if vulnerabilities are effectively addressed
- (D) Change all user passwords across the organization

Question 252. A Security Analyst at BetaTech is reviewing the monitoring tools deployed across the organization. She wants to ensure that every tool can detect unauthorized changes made to system files and configurations. Which of the following tools is BEST suited for this purpose?

- (A) Network protocol analyzer
- (B) File integrity monitoring (FIM) system
- (C) Bandwidth monitoring tool
- (D) Passive vulnerability scanner

Question 253. An e-commerce company wants to ensure that their customers' credit card data remains confidential while in transit over the internet. They are seeking a protocol that can help in securing their website's communication. Which protocol would best fit this requirement?

- (A) IPSec
- (B) SSH
- (C) TLS
- (D) ICMP

Question 254. After a recent security breach, Sarah, a cybersecurity analyst, is implementing additional measures to detect unauthorized activities. She decides to embed specific values in the database that serve no real purpose but are monitored for any unauthorized access or usage. These values are designed to raise alerts if they are ever accessed or used. What are these specific values commonly referred to as?

- (A) Security flags
- (B) Honeypots
- (C) Honeytokens
- (D) Audit trails

Question 255. Maria receives a text message on her phone from an unknown number, stating that she has won a gift card worth \$500 from a popular online store. The message includes a link asking her to click on it to claim her prize. Maria is unsure

about the authenticity of the message. Which of the following is the BEST course of action for Maria?

- (A) Click the link to check if the website looks genuine
- (B) Forward the message to her friends to verify if they received a similar message
- (C) Delete the message without clicking on any links
- (D) Respond to the sender asking for more details about the offer

Question 256. At AlphaTech, the security team is assessing vulnerabilities in a newly deployed cloud infrastructure. While analyzing potential risks, they consider factors such as the physical location of data centers, local laws and regulations, and natural disaster frequencies. What are these considerations known as in the context of vulnerability management?

- (A) Asset valuation factors
- (B) Risk response variables
- (C) Threat intelligence variables
- (D) Environmental variables

Question 257. During an e-commerce website audit, a security analyst discovers that if a user tries to purchase a product and simultaneously cancels the order, the product sometimes gets added to the user's cart without deducting any funds. This vulnerability can potentially be exploited to obtain products for free. Which vulnerability type is the e-commerce website susceptible to?

- (A) Directory Traversal
- (B) Insecure Direct Object References (IDOR)
- (C) Race Condition
- (D) Cross-Site Request Forgery (CSRF)

Question 258. XYZ Corp., a multinational company, recently underwent a security audit. The Chief Information Security Officer (CISO) needs to report the findings of the audit to the company's internal stakeholders as well as to a governmental regulatory agency. Which of the following represents the correct type of compliance reporting for each recipient?

- (A) Internal report for the regulatory agency and external report for internal stakeholders
- (B) External report for both the regulatory agency and internal stakeholders
- (C) Internal report for internal stakeholders and external report for the regulatory agency
- (D) No report is required for internal stakeholders, only an external report for the regulatory agency

Question 259. During a critical financial quarter, GlobalFin Corp experienced unexpected outages during peak business hours due to system maintenance, impacting its operations significantly. To prevent such occurrences in the future, what should GlobalFin Corp implement regarding their maintenance activities?

- (A) Conduct maintenance activities randomly to avoid predictability
- (B) Implement maintenance activities during peak business hours
- (C) Establish designated maintenance windows
- (D) Reduce the frequency of maintenance activities

Question 260. Alex, a new intern at an IT company, wanted to access the internal company portal. Instead of typing "companyportal.com," he accidentally typed

“comapnyportal.com” and ended up on a site that looked identical but asked him to download a security certificate. This scenario best describes which type of attack?

- (A) Spear Phishing
- (B) Watering Hole Attack
- (C) Typosquatting
- (D) Man-in-the-Middle

Question 261. DataGuard Corp. operates in the European Union and has recently suffered a major data breach affecting the personal data of thousands of users. They failed to comply with some key provisions of the General Data Protection Regulation (GDPR). Which of the following is the MOST likely immediate consequence of their non-compliance?

- (A) They will be forced to shut down operations until compliance is achieved
- (B) DataGuard's executive team will face immediate imprisonment
- (C) The company will be required to issue a public apology
- (D) DataGuard Corp. will face substantial fines for their non-compliance

Question 262. A pharmaceutical company is working on a new drug formula that promises to revolutionize the treatment of a particular disease. The R&D team has detailed documentation on the components, procedures, and results of the drug trials. How should this documentation be classified to ensure that only the right people within the company have access?

- (A) Unclassified
- (B) Public

- (C) Confidential
- (D) Sensitive

Question 263. After a recent software update, a company's intranet portal has been inaccessible to a few employees. The IT team suspects it could be due to network filtering rules. What should the IT team review to confirm their suspicions?

- (A) The content filtering policies
- (B) The malware detection logs
- (C) The allow list/deny list configurations
- (D) The network bandwidth utilization graphs

Question 264. MegaCorp recently introduced a new web application for its customers. Before its release, the software underwent rigorous testing in a controlled environment. When the application was deployed in production, several security vulnerabilities were reported. Which of the following reasons can explain the mismatch between the test results and actual vulnerabilities?

- (A) The testing environment was an exact replica of the production environment
- (B) Test results were not thoroughly reviewed
- (C) The software was not tested for zero-day vulnerabilities
- (D) Penetration testing was done post-production

Question 265. NexTech, a cloud-based software company, recently faced a security breach due to inconsistent practices among its system administrators. To avoid such inconsistencies in the future, what should NexTech emphasize in its operations?

- (A) Rely on system administrators to develop their

personal methods

- (B) Mandate frequent system reboots
- (C) Implement Standard Operating Procedures (SOPs) for all technical operations
- (D) Conduct random security audits without notifying administrators

Question 266. After running a vulnerability scan on the company's infrastructure, a security analyst notices a reported vulnerability on a server. However, after manual verification, the analyst determines that the vulnerability doesn't actually exist on the server. What is this situation best described as?

- (A) A false negative
- (B) A true positive
- (C) A false positive
- (D) A confirmation bias

Question 267. Your organization has been repeatedly ignoring the security guidelines set forth by a global standards organization, despite having pledged adherence. Given the repetitive nature of these violations, the organization is now facing disciplinary measures. Which of the following is the MOST likely immediate consequence of these actions?

- (A) Immediate revocation of business licenses
- (B) Sanctions imposed by the global standards organization
- (C) Forcible shutdown of all online operations for a determined period
- (D) Mandatory public apology to stakeholders

Question 268. Sophia, the cybersecurity lead at XYZ Corp, is in the process of drafting a new security policy. During the drafting process, she primarily consults with her security team. However, upon implementation, several departments pushed back due to the policy interfering with their operations. Which best describes the misstep Sophia made during the policy creation process?

- (A) Not using a standardized security framework
- (B) Over-reliance on automated security solutions
- (C) Not including key stakeholders in the policy drafting process
- (D) Focusing too much on external threats rather than internal ones

Question 269. A company's network administrator notices that several switches in the network infrastructure are no longer receiving firmware updates from the manufacturer. These devices are no longer sold or supported. What vulnerability do these switches introduce to the network?

- (A) Physical hardware tampering
- (B) Lack of redundancy
- (C) Increased susceptibility to new threats
- (D) Wireless interference

Question 270. Liam, the CTO of a medium-sized enterprise, noticed that several software applications were not updated regularly, leading to potential security vulnerabilities. Upon investigation, he realized that no specific team or individual was assigned as the owner of these applications. To enhance security, what should Liam emphasize?

- (A) Immediate decommissioning of all unowned

applications

- (B) Assignment of clear ownership to all business applications
- (C) Conducting monthly vulnerability assessments on all applications
- (D) Outsourcing the management of these applications to third-party vendors

Question 271. Sophia received an email from her bank asking her to urgently update her personal details due to a system upgrade. The email contains a link that redirects to a website that looks similar to her bank's website. Which of the following should she do FIRST?

- (A) Follow the link and promptly update her personal details to avoid any inconvenience
- (B) Forward the email to her friends and family to ensure they are also aware of the bank's system upgrade
- (C) Delete the email immediately without taking any action
- (D) Contact her bank through official channels to verify the authenticity of the email

Question 272. AlphaTech, a growing SaaS company, has multiple applications deployed across different cloud providers. The security team struggles to manage and analyze logs from these disparate sources. Which solution would BEST help AlphaTech centralize their logs for a more streamlined analysis?

- (A) Network Intrusion Detection System (NIDS)
- (B) Log Aggregation Tool
- (C) Data Loss Prevention (DLP) software
- (D) Vulnerability Scanner

Question 273. AlphaTech is seeking a comprehensive source of intelligence about the latest cyber threats targeting its specific industry. While OSINT provides valuable data, the company is considering investing in a more specialized solution. Which of the following would best address AlphaTech's needs?

- (A) Implementing internal honeypots to trap attackers
- (B) Subscribing to a third-party threat intelligence feed
- (C) Regularly attending cyber security conferences
- (D) Using open-source vulnerability scanners

Question 274. An employee receives a call from someone claiming to be from the IT department. The caller says there's an urgent update required on the employee's computer and asks for login credentials to perform the update remotely. The employee becomes suspicious because of which red flag regarding impersonation?

- (A) The caller did not use technical jargon
- (B) IT normally sends email notifications about updates
- (C) The employee was not expecting any updates
- (D) The caller's voice sounded unfamiliar

Question 275. As a security consultant, you are hired by a multinational corporation to assess the security posture of their potential vendors. One of the vendors appears promising, but your client wants to ensure that the vendor periodically examines and strengthens its own internal procedures and security controls. What should you advise your client to request from this vendor?

- (A) The vendor's business continuity plan
- (B) A list of the vendor's clients

- (C) Evidence of internal audits
- (D) The vendor's company mission statement

Question 276. TechDynamics, a growing tech startup, plans to scale its operations and serve a global clientele. Given that their client base operates in multiple time zones, when should TechDynamics schedule their system maintenance to ensure minimal disruption?

- (A) During the busiest hours for their headquarters' local time
- (B) Staggered based on the peak hours of their global clients
- (C) Only when a system breakdown occurs
- (D) Establish a consistent maintenance window during off-peak hours for the majority of their clientele

Question 277. A defense contractor is working on a new missile system. While the detailed schematics and operational details are classified, they have an overview document that only a select group of partners and stakeholders can view. How should this overview document be classified?

- (A) Public
- (B) Restricted
- (C) Confidential
- (D) Top Secret

Question 278. TechFusion and CodeRush, two independent software development companies, are collaborating on a project that is expected to define industry standards for a new coding language. While both parties have an understanding of shared responsibilities, they have not yet established legally binding

obligations. Which type of agreement best suits their current collaborative understanding?

- (A) Service-level agreement (SLA)
- (B) Non-disclosure agreement (NDA)
- (C) Memorandum of agreement (MOA)
- (D) Licensing agreement

Question 279. A security analyst at CyberSecure Corp. reviews a vulnerability report concerning an application that could allow attackers to upload malicious scripts. Once these scripts are executed, they can grant attackers complete control over the application. How should this vulnerability be primarily classified?

- (A) Integrity vulnerability
- (B) Availability vulnerability
- (C) Remote code execution vulnerability
- (D) Disclosure vulnerability

Question 280. A financial institution is updating its infrastructure to ensure that customer financial data is kept secure from both internal and external threats. Which of the following would be the MOST effective measure to protect customer financial data from being accessed by unauthorized internal users?

- (A) Deploying perimeter firewalls around the institution's network
- (B) Implementing two-factor authentication (2FA) for all customer accounts
- (C) Enforcing strict access controls based on the principle of least privilege

(D) Conducting yearly cybersecurity awareness training for all employees

Question 281. Alice, a system administrator for a startup, is preparing to deploy a new website for her company. To ensure secure communications between the users and the website, she plans to obtain a digital certificate for the site. Before doing so, which step must Alice first undertake to get a certificate from a Certificate Authority (CA)?

- (A) Generate a public-private key pair
- (B) Submit her passport copy to the CA
- (C) Download the latest CA root certificate
- (D) Encrypt the website with symmetric encryption

Question 282. TechFin Bank is considering implementing a new software system for their transaction processing. Before rolling it out, the cybersecurity team insists on carrying out a specific type of analysis to understand how this change might affect the organization's security posture. What is the team referring to?

- (A) Risk appetite assessment
- (B) Performance benchmarking
- (C) Impact analysis
- (D) Penetration testing

Question 283. The software development team at ABC Corp. has created a unique application that utilizes innovative algorithms. The company wants to ensure that competitors cannot legally copy or replicate their application's functionality. Which of the following would be the MOST suitable method to protect this intellectual property?

- (A) Copyright the user interface design
- (B) Apply for a patent for the innovative algorithms
- (C) Store the application code in an encrypted vault
- (D) Ensure all users sign an acceptable use policy (AUP)

Question 284. SecureBank is in the process of selecting a vendor for their new online transaction system. The bank is keen on ensuring the selected vendor has robust security measures and a track record of maintaining those measures. As part of the vendor selection process, which of the following steps is the most relevant to the bank's concerns?

- (A) Checking the vendor's sales growth over the last five years
- (B) Conducting due diligence regarding the vendor's security practices
- (C) Comparing the visual appeal of the vendor's user interface to competitors
- (D) Evaluating the vendor's marketing strategies

Question 285. XYZ Corp, a manufacturer of smart home devices, failed to implement standard security practices in their products. A popular tech review site publishes an in-depth review detailing these vulnerabilities. Which of the following outcomes is XYZ Corp MOST likely to face as an immediate result?

- (A) An award for innovation in smart home technologies
- (B) Reputational damage leading to decreased sales
- (C) An increased partnership with tech retailers
- (D) A surge in the employee recruitment rate

Question 286. An e-commerce company is experiencing attacks that specifically target the shopping cart feature of its web application. They want to implement a firewall that can understand web application-specific commands and provide protection. Which type of firewall should they consider?

- (A) Layer 4 Firewall
- (B) Layer 2 Firewall
- (C) Layer 7 Firewall
- (D) Packet Filtering Firewall

Question 287. John, a senior executive at XYZ Corp., gets a call from someone claiming to be from the bank's fraud department. The caller asks John to confirm certain transactions by providing the OTP sent to his registered mobile number. What form of social engineering attack is John likely facing?

- (A) Baiting
- (B) Quizzing
- (C) Vishing
- (D) Pharming

Question 288. DeltaCorp, a retail company, has assessed that a security breach might result in a loss of \$1 million in sales. The company has determined that they can tolerate a loss of up to \$500,000, but anything beyond that would severely impact operations. To cover the potential financial loss beyond their tolerance level, they decide to purchase cybersecurity insurance. Which of the following terms best describes the \$500,000 figure?

- (A) Risk appetite
- (B) Risk threshold

- (C) Risk capacity
- (D) Risk assessment

Question 289. A financial organization collects and stores personally identifiable information (PII) of its customers. The company operates within jurisdictions that have strict regulations concerning the storage, transmission, and processing of such data. Which of the following strategies would be MOST appropriate for the company to ensure compliance with these regulations?

- (A) Use open source encryption algorithms without validation
- (B) Only store customer data in physical, on-site servers
- (C) Implement data classification and labeling procedures
- (D) Limit the number of administrators with access to the data

Question 290. An organization is transitioning its IT infrastructure to be cloud-centric and aims to adopt a zero-trust network approach. They are looking for a solution that integrates cloud security, zero-trust access, and WAN capabilities, ensuring employees have consistent secure access regardless of their location. Which of the following best addresses their needs?

- (A) Remote Desktop Services (RDS)
- (B) Secure access service edge (SASE)
- (C) Content Delivery Network (CDN)
- (D) Virtual Local Area Network (VLAN)

Question 291. MedTech, a medical device manufacturer, did not adhere to the required standards for device security and patient data protection. Which of the following repercussions might be the MOST critical for MedTech's ongoing operations?

- (A) Increased public relations campaigns
- (B) Short-term stock price fluctuations
- (C) Offering discounts on their devices
- (D) Loss of license to manufacture and distribute

Question 292. A multinational corporation is looking to replace its current firewalls at all its global branches. The IT director wants a solution that can perform stateful inspection of packets, application-level filtering, and integrate threat intelligence feeds for updated threat awareness. Which of the following would be the most suitable solution?

- (A) Stateful Packet Inspection Firewall
- (B) Proxy Server
- (C) Web Application Firewall (WAF)
- (D) Next-Generation Firewall (NGFW)

Question 293. A security analyst is reviewing a vulnerability report and sees a reference to CVE-2023-12345 with a CVSS score of 9.5. Which of the following conclusions can the analyst draw based on this information?

- (A) The vulnerability was first identified in the year 2023
- (B) The vulnerability is of low severity
- (C) The vulnerability affects only software produced in 2023
- (D) CVE-2023-12345 is the software vendor's internal code for the vulnerability

Question 294. GlobalTech, a software development company, is entering into a partnership with WebSolutions, a web hosting provider. They aim to create a standard set of terms governing their ongoing business transactions, including payment terms, delivery protocols, and warranties. Which type of agreement is most suitable for establishing these foundational terms for future transactions?

- (A) Memorandum of understanding (MOU)
- (B) Non-disclosure agreement (NDA)
- (C) Licensing agreement
- (D) Master service agreement (MSA)

Question 295. AlphaTech, a leading IT company, recently identified a critical vulnerability in its primary software product. They have developed a patch to address the vulnerability. Before distributing the patch to its customers, which of the following should AlphaTech ideally perform?

- (A) Deploy the patch on all company systems
- (B) Notify the media about the vulnerability
- (C) Test the patch in a controlled environment
- (D) Offer compensation to affected customers

Question 296. Employees at a renowned software development firm frequently visit an industry-related forum to discuss the latest trends and technologies. Over the past month, several employees reported malware infections shortly after accessing the forum. An investigation suggests the forum was compromised to target the company's developers specifically. Which type of attack most accurately describes this scenario?

- (A) Spear Phishing
- (B) Watering Hole

- (C) Drive-by Download
- (D) Whaling

Question 297. A cybersecurity firm has been hired by TechGiant Corp. to perform penetration testing on their infrastructure. Before the testing begins, the CEO of TechGiant Corp. wants to ensure that certain critical systems are not targeted, and that the testing will not disrupt their ongoing operations. What should be established to define the scope and boundaries of the test?

- (A) Service-level agreement (SLA)
- (B) Non-disclosure agreement (NDA)
- (C) Rules of engagement (ROE)
- (D) Memorandum of understanding (MOU)

Question 298. During a routine vulnerability assessment, TechInc discovers a weakness in their system that, if exploited, would allow an attacker to modify existing user accounts, including privileges. Which classification best describes this vulnerability?

- (A) Elevation of privilege vulnerability
- (B) Disclosure vulnerability
- (C) Replay vulnerability
- (D) Remote code execution vulnerability

Question 299. An e-commerce company is rolling out a new web application to facilitate online payments. The IT department wants to be immediately notified of any application errors or unauthorized modifications to the application's codebase. Which of the following tools should they implement?

- (A) Web Application Firewall (WAF)

- (B) Application Performance Monitoring (APM)
- (C) Domain Name System (DNS) monitoring tool
- (D) Network flow analyzer

Question 300. A security analyst is exploring ways to proactively identify vulnerabilities within the organization's infrastructure. Which of the following provides the BEST method for the analyst to receive real-time threat intelligence from the dark web?

- (A) Utilizing a vulnerability scanner on the organization's internal network
- (B) Subscribing to a dark web threat intelligence feed
- (C) Conducting regular penetration tests on external-facing systems
- (D) Reviewing daily reports from the organization's SIEM system

Answers 201-300

Question 201. An international bank is setting up a new online portal for its customers to access their financial statements. Which measure should the bank implement to ensure that financial data in transit between the customer's browser and the bank's servers is kept confidential?

- (A) Use file-level encryption for all financial statements
- (B) Implement a Web Application Firewall (WAF)

- (C) Use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for the portal
- (D) Store all financial data in an encrypted database

Explanation 201. Correct Answer: C. Use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for the portal. SSL/TLS is designed to secure data in transit. By encrypting the data between the customer's browser and the bank's servers, it ensures the data's confidentiality while in transit.

Option A is incorrect. File-level encryption is great for data at rest but doesn't secure data in transit between a client and server.

Option B is incorrect. While a WAF can provide protection against web application attacks, it does not inherently encrypt data in transit.

Option D is incorrect. Storing financial data in an encrypted database safeguards the data at rest but doesn't ensure the confidentiality of data in transit to the client.

Question 202. A multinational organization with multiple branch offices is looking to simplify their WAN connectivity and reduce costs while ensuring that their inter-office data transfers remain secure. Which technology would best fit their needs?

- (A) VLAN
- (B) MPLS

- (C) SD-WAN
- (D) DMZ

Explanation 202. Correct Answer: C. SD-WAN. Software-defined wide area network (SD-WAN) offers enterprises the ability to leverage any combination of transport services, including MPLS, LTE, and broadband internet services, to securely connect users to applications. SD-WAN can reduce costs by enabling the use of lower-cost internet connections and can also simplify WAN management.

Option A is incorrect. VLAN (Virtual Local Area Network) is used to segment a local network into different broadcast domains, but it does not facilitate WAN connectivity or reduce WAN costs.

Option B is incorrect. MPLS (Multi-Protocol Label Switching) is a type of WAN technology that can be expensive. While it provides reliable and fast connections, it doesn't offer the cost-saving benefits or flexibility of SD-WAN.

Option D is incorrect. DMZ (Demilitarized Zone) is a buffer zone between an organization's internal network and the external, untrusted networks. It is not related to WAN connectivity or cost reduction.

Question 203. While setting up a new internal web application, Laura, a system administrator, decides to use a digital certificate for SSL/TLS encryption. Due to budget constraints, she can't procure a certificate from a commercial Certificate Authority (CA). Which of the following would be a viable option for

Laura to secure the application?

- (A) Rely on plaintext HTTP for the application
- (B) Obtain a certificate from a free Certificate Authority
- (C) **Generate a self-signed certificate**
- (D) Use a shared certificate from another application

Explanation 203. Correct Answer: C. Generate a self-signed certificate. A self-signed certificate can be generated by Laura without the need for a Certificate Authority. While self-signed certificates can cause trust issues in public-facing applications (since they aren't signed by a recognized CA), they can be appropriate for internal applications where users can be informed and trust can be established manually.

Option A is incorrect. Relying on plaintext HTTP doesn't provide any encryption or security for the application, leaving it vulnerable to various attacks.

Option B is incorrect. While obtaining a certificate from a free Certificate Authority is a valid option, it wasn't the best choice given the specific scenario which emphasizes not using a CA.

Option D is incorrect. Using a shared certificate from another application can introduce security risks and is not a recommended practice.

Question 204. A renowned technology company recently released a new line of routers. After a short period, security researchers discovered that some of these routers contain malicious chips embedded during the manufacturing process. This incident most likely represents a vulnerability related to

which supply chain aspect?

- (A) Outsourced software development risks
- (B) Service provider's outdated security practices
- (C) **Hardware provider's embedded compromise**
- (D) Inadequate vendor background checks

Explanation 204. Correct Answer: C. Hardware provider's embedded compromise. Supply chain vulnerabilities in the context of hardware providers can involve the introduction of malicious components or chips during the manufacturing process. In this scenario, the presence of malicious chips in the routers is a direct reflection of a vulnerability due to a compromised hardware provider.

Option A is incorrect. The scenario revolves around a hardware compromise, not software development outsourcing.

Option B is incorrect. While it's essential for service providers to employ up-to-date security practices, the vulnerability in this scenario is attributed to a hardware compromise and not outdated security practices.

Option D is incorrect. Although vendor background checks are important, this scenario emphasizes a vulnerability stemming from the hardware manufacturing process, not the vetting process of vendors.

Question 205. A multinational corporation is expanding its operations in various countries. The company has decided to restrict access to its internal network based on geolocation to ensure that only employees from specific countries can access

certain data. Which of the following would be the MOST appropriate solution to implement this requirement?

- (A) Deploy a VPN with multi-factor authentication
- (B) Use MAC address filtering on all company devices
- (C) **Implement a geolocation-based access control system**
- (D) Set up region-specific SSIDs for the company's Wi-Fi network

Explanation 205. Correct Answer: C. Implement a geolocation-based access control system. Geolocation-based access control systems determine users' physical locations and can grant or deny access based on predefined geographic boundaries. This solution is most fitting for restricting access based on country-specific requirements.

Option A is incorrect. While a VPN with multi-factor authentication improves security, it doesn't inherently restrict access based on geolocation.

Option B is incorrect. MAC address filtering restricts access based on device hardware addresses and not on geolocation.

Option D is incorrect. Region-specific SSIDs might limit Wi-Fi access in certain areas, but they don't enforce geolocation-based restrictions on a broader scale.

Question 206. TechGuard Inc. and CloudSecure are two cybersecurity firms that are considering a collaboration on a new cloud security project. Both companies have proprietary technologies and methodologies they will bring into the

partnership. Before embarking on the collaborative venture, which agreement should they finalize to define the terms of their partnership, roles, and shared responsibilities?

- (A) Non-disclosure agreement (NDA)
- (B) Service-level agreement (SLA)
- (C) **Business partners agreement (BPA)**
- (D) Memorandum of understanding (MOU)

Explanation 206. Correct Answer: C. Business partners agreement (BPA). A Business partners agreement (BPA) outlines the specifics of the partnership between entities, detailing roles, responsibilities, financial arrangements, and other key terms of the relationship. Given that TechGuard Inc. and CloudSecure are forming a partnership with shared roles and responsibilities, a BPA is the most fitting.

Option A is incorrect. An NDA focuses specifically on the confidentiality of shared information and not on the broader terms of a partnership.

Option B is incorrect. A service-level agreement (SLA) centers on the standards and quality of service to be provided, detailing performance metrics, and does not focus on partnership specifics.

Option D is incorrect. An MOU signifies mutual intentions and understanding between parties but may not provide detailed terms and conditions of a business partnership like a BPA does.

Question 207. A security team recently upgraded their intrusion detection system (IDS). Since the upgrade, the system hasn't

flagged any intrusions, even though intrusion attempts are a regular occurrence. What is this situation best characterized as?

- (A) A true negative
- (B) **A false negative**
- (C) A true positive
- (D) A confirmation feedback

Explanation 207. Correct Answer: B. A false negative. A false negative occurs when a system fails to detect a threat or vulnerability that is actually present. In this scenario, the IDS isn't detecting real intrusion attempts, which could lead to undetected breaches.

Option A is incorrect. A true negative would mean that the system correctly identified that there were no intrusions when there truly weren't any. This isn't the scenario described as intrusion attempts are expected.

Option C is incorrect. A true positive means that the threat or vulnerability was correctly identified and truly exists. Since no intrusions are being detected, this isn't a true positive.

Option D is incorrect. "Confirmation feedback" isn't a standard term related to vulnerability detection and doesn't apply to the described scenario.

Question 208. CyberTech Inc., a cybersecurity consulting company, is in discussions with a potential client, MedCorp, to assist in developing a new secure medical records system. MedCorp will be sharing sensitive patient data with CyberTech as part of the process. Which agreement should be in place

before the sharing of such information to ensure confidentiality?

- (A) Memorandum of understanding (MOU)
- (B) Service-level agreement (SLA)
- (C) **Non-disclosure agreement (NDA)**
- (D) Work order (WO)/statement of work (SOW)

Explanation 208. Correct Answer: C. Non-disclosure agreement (NDA). An NDA (Non-disclosure agreement) is specifically designed to safeguard confidential information that is shared between two parties. It ensures that the receiving party doesn't disclose or misuse the information provided. Given the sensitive nature of the patient data that MedCorp will share, an NDA is crucial.

Option A is incorrect. An MOU signifies mutual intentions and understanding between parties but doesn't specifically cater to the confidentiality of shared information.

Option B is incorrect. A service-level agreement (SLA) is primarily about the level of service to be provided, detailing performance metrics, and penalties for non-compliance. It doesn't inherently focus on data confidentiality.

Option D is incorrect. A Work order (WO) or statement of work (SOW) details the specifics of a project, from tasks to milestones, but doesn't directly address the confidentiality of shared data.

Question 209. While analyzing server logs, Mike, an IT security analyst, noticed that an unfamiliar document was frequently accessed. Upon investigation, he realized that this

document was deliberately placed by the security team and had no real data but was closely monitored. The purpose of this file is MOST likely:

- (A) To serve as a redundancy copy in case of data loss
- (B) **To act as a decoy to attract and detect unauthorized access**
- (C) To maintain a record of all user activities for auditing
- (D) To be encrypted and sent to clients as a sample

Explanation 209. Correct Answer: B. To act as a decoy to attract and detect unauthorized access. Honeyfiles serve as deceptive measures, attracting potential malicious actors or unauthorized users. If such files are accessed, it can be an indication of unauthorized or suspicious activities in the system.

Option A is incorrect. Redundancy copies or backups are created to prevent data loss due to unforeseen issues, but they are not monitored as decoys.

Option C is incorrect. User activity logs maintain records of actions taken within a system or application, which is different from a deceptive measure like a honeyfile.

Option D is incorrect. Files encrypted for client samples serve a different purpose and are not typically used as decoys to detect unauthorized access.

Question 210. After implementing a major security update to its database system, TechCo experienced unexpected downtime and system incompatibilities. The CISO wants to ensure that such incidents can be quickly addressed in the future. Which of

the following should TechCo have had in place before deploying the update to mitigate the impact of these kinds of incidents?

- (A) A comprehensive list of all updates
- (B) An automated system recovery tool
- (C) **A backout plan**
- (D) A detailed user manual for the update

Explanation 210. Correct Answer: C. A backout plan. A backout plan is a pre-arranged strategy or set of procedures to reverse changes made to the system in case the changes have adverse effects. In scenarios like this, where a significant update causes unintended problems, a backout plan would allow the organization to revert the system to its previous stable state quickly.

Option A is incorrect. While having a comprehensive list of all updates is good for documentation and auditing purposes, it would not directly help in mitigating the effects of an adverse update.

Option B is incorrect. An automated system recovery tool might assist in reverting changes or recovering the system. However, a backout plan is more specific to undoing changes made during an update or change process, making it more suitable in this context.

Option D is incorrect. A detailed user manual for the update is beneficial for training and troubleshooting, but it wouldn't serve the direct purpose of reverting unintended adverse changes.

Question 211. TechFirm is preparing to embark on a new project with a client, focusing on implementing a cybersecurity infrastructure overhaul. They wish to lay out the specific tasks, deliverables, timelines, and resources required for this project. Which type of agreement would best capture these details?

- (A) Memorandum of understanding (MOU)
- (B) Joint venture agreement
- (C) Master service agreement (MSA)
- (D) **Work order (WO)/statement of work (SOW)**

Explanation 211. Correct Answer: D. Work order (WO)/statement of work (SOW). A Work order (WO) or statement of work (SOW) is tailored to outline the specifics of a particular job or project. It often includes details such as tasks, deliverables, schedules, and necessary resources. Given that TechFirm seeks to describe the details of their cybersecurity overhaul project, the WO/SOW is the most appropriate choice.

Option A is incorrect. An MOU is a more general agreement signifying mutual intentions, but it doesn't delve into specific tasks or deliverables of a particular project.

Option B is incorrect. A joint venture agreement is mainly concerned with the creation of a new entity or project involving multiple parties, highlighting their roles and responsibilities.

Option C is incorrect. A Master service agreement (MSA) provides a broad framework covering the terms and conditions of business transactions between parties. It doesn't specify details of individual projects.

Question 212. The IT department of a large corporation is performing a vulnerability assessment on its virtualized infrastructure. They come across a potential threat where a user from within a VM can interact and possibly compromise the host system. What is this type of vulnerability commonly referred to as?

- (A) VM cloning
- (B) VM snapshotting
- (C) **VM escape**
- (D) VM migration

Explanation 212. Correct Answer: C. VM escape. A VM escape occurs when an attacker runs code on a VM that allows them to break out of the VM's isolated environment and gain access to the host system.

A virtual machine (VM) escape refers to the exploitation of a vulnerability in the virtualization software, allowing an attacker who has control over a VM to break out of its isolated environment and gain access to the host system. This can lead to the potential compromise of other VMs running on the same host or the underlying infrastructure.

Option A is incorrect. VM cloning is the process of creating an exact copy of a VM. It does not involve breaking out of the VM's isolated environment.

Option B is incorrect. VM snapshotting involves creating a point-in-time copy of a VM, which can be used for backup or recovery purposes. It is not related to escaping from a VM.

Option D is incorrect. VM migration refers to the process of moving a VM from one host to another, often for load balancing or hardware maintenance. It does not involve escaping from the VM's isolated environment.

Question 213. A large organization is considering deploying a solution that will allow employees to securely access company resources remotely using their personal devices. The organization wants a solution that can provide strong authentication and ensure that the data remains confidential during transit. Which technology should be adopted?

- (A) Kerberos
- (B) Remote Desktop Services (RDS)
- (C) **Remote Access VPN**
- (D) SNMP

Explanation 213. Correct Answer: C. Remote Access VPN. Remote Access VPN provides a secure connection from a remote device to an organization's internal network. It uses encryption to ensure data confidentiality and can also be set up with strong authentication methods.

Option A is incorrect. Kerberos is an authentication protocol that uses tickets to allow nodes to prove their identity in a network. While it provides strong authentication, it doesn't inherently provide a solution for remote access with encrypted communication.

Option B is incorrect. Remote Desktop Services (RDS) allows users to access a remote desktop or application. While it can be

secured, it doesn't always ensure encryption during transit, especially if not paired with another technology like VPN.

Option D is incorrect. SNMP (Simple Network Management Protocol) is used for managing and monitoring network devices. It isn't related to providing secure remote access for users.

Question 214. A security analyst at ZetaTech is looking to gather information about emerging threats and vulnerabilities relevant to their industry. Which of the following would be the MOST suitable method to obtain real-time, continuously updated data on potential security issues?

- (A) Relying solely on automated internal vulnerability scanners
- (B) Periodic manual penetration testing
- (C) **Subscribing to an OSINT threat feed**
- (D) Regularly checking the company's firewall logs

Explanation 214. Correct Answer: C. Subscribing to an OSINT threat feed. An OSINT (Open-source intelligence) threat feed provides real-time information and is continuously updated with data on potential security issues sourced from publicly available information.

Option A is incorrect. While automated internal vulnerability scanners are valuable for identifying vulnerabilities within the organization's infrastructure, they don't provide continuous real-time data about external emerging threats.

Option B is incorrect. Manual penetration testing is periodic and doesn't offer continuous updates on emerging threats from the broader industry.

Option C is incorrect. Regularly checking the company's firewall logs will give insight into potential malicious activities targeting the company, but it won't offer broad, updated data on industry-wide threats.

Question 215. While conducting a security assessment, Lucy found that a specific application crashes when she inputs a string that is much longer than what the input field is designed to handle. This could potentially allow her to execute arbitrary code in the application's context. What vulnerability is Lucy likely trying to exploit?

- (A) SQL Injection
- (B) Cross-Site Scripting (XSS)
- (C) **Buffer Overflow**
- (D) Directory Traversal

Explanation 215. Correct Answer: C. Buffer Overflow.

Buffer overflow vulnerabilities occur when data written to a buffer exceeds that buffer's boundaries, potentially overwriting adjacent memory locations. If exploited successfully, it can lead to arbitrary code execution.

Buffer overflow is a condition where an application writes more data to a buffer than it can hold, causing the excess data to overflow into adjacent memory spaces. When this happens, attackers can overwrite specific parts of the memory, which

may lead to arbitrary code execution, application crashes, or data corruption.

Option A is incorrect. SQL Injection involves injecting malicious SQL statements into an entry field for execution, aiming to manipulate a database. It doesn't relate to buffer boundaries or memory overflows.

Option B is incorrect. Cross-Site Scripting (XSS) allows attackers to inject malicious scripts into web pages viewed by other users. While this is an input validation flaw like a buffer overflow, XSS specifically targets script execution within web browsers and does not involve overflowing buffer boundaries.

Option D is incorrect. Directory Traversal attacks aim to access files and directories stored outside the web root folder. They don't involve overflowing buffer boundaries or memory overflows.

Question 216. WebFirm, a web development company, did not comply with the data handling and protection clauses outlined in their contract with RetailMax, an e-commerce company. As a result, RetailMax's customer data was exposed in a data breach. Which of the following is the MOST probable contractual impact on WebFirm due to this incident?

- (A) WebFirm will receive bonuses for early project completion
- (B) WebFirm will be required to provide additional services at no cost
- (C) **RetailMax will terminate the contract and may**

seek damages

(D) RetailMax will extend the project timeline

Explanation 216. Correct Answer: C. RetailMax will terminate the contract and may seek damages. A data breach, especially one that results from non-compliance with contractual clauses related to data protection, can lead to the termination of the contract. Additionally, the affected party, in this case, RetailMax, might also seek damages from WebFirm for the breach.

Option A is incorrect. Bonuses for early project completion are unrelated to non-compliance with data protection clauses.

Option B is incorrect. While some contracts might stipulate penalties such as providing additional services for breaches, in a significant incident like a data breach, termination is more probable.

Option D is incorrect. Extending the project timeline is not a typical response to a breach of data protection clauses in a contract.

Question 217. During a political campaign, an anonymous group releases a series of articles containing fabricated data about a candidate's past, intending to influence voters' opinions. This is an example of:

- (A)** Impersonation
- (B)** SSmishing
- (C) Disinformation**
- (D)** Baiting

Explanation 217. Correct Answer: C. Disinformation. The spread of deliberately false information to deceive or harm, especially in sensitive areas like politics, is classified as disinformation.

Disinformation campaigns aim to deceive audiences by presenting false information as if it's true. In political scenarios, this can have significant ramifications, affecting public opinion and the outcome of elections.

Option A is incorrect. Impersonation involves pretending to be someone else to deceive, but the scenario doesn't indicate that the anonymous group is impersonating anyone.

Option B is incorrect. Smishing is a type of phishing attack that uses SMS. It doesn't relate to spreading false information in articles.

Option D is incorrect. Baiting involves enticing victims with something they want (like free software) to steal their personal information or to spread malware. It doesn't involve the spread of false information as described in the scenario.

Question 218. A multinational company is considering using a cloud storage provider based in a foreign country to store customer data. The company's home country has strict data protection laws that require customer data to remain within its borders. Which of the following considerations is MOST critical for the company when choosing the cloud storage provider?

(A) The speed of data access from the foreign-based cloud

storage

(B) The encryption standards used by the foreign cloud provider

(C) Whether the foreign cloud provider offers data storage exclusively within the company's home country

(D) The reputation and customer reviews of the foreign cloud provider

Explanation 218. Correct Answer: C. Whether the foreign cloud provider offers data storage exclusively within the company's home country. Data sovereignty refers to the concept that digital data is subject to the laws of the country in which it is located. If a company's home country has regulations that require customer data to stay within its borders, it's essential to ensure that the cloud provider offers storage that complies with this requirement.

Option A is incorrect. While speed of data access is important, it doesn't address the data sovereignty concern.

Option B is incorrect. While encryption is essential for security, it doesn't guarantee compliance with data sovereignty laws.

Option D is incorrect. Reputation is important, but it doesn't directly address the specific requirement of data sovereignty.

Question 219. BetaTech, a tech manufacturing firm, wants to ensure that a potential compromise of its IoT devices will not endanger its primary manufacturing control systems. Which of the following approaches would be most effective in achieving

this?

- (A) Using a single robust firewall for the entire network
- (B) Periodic password changes for IoT devices
- (C) **Segmenting the IoT devices from the manufacturing control systems**
- (D) Enabling automatic updates for all IoT devices

Explanation 219. Correct Answer: C. Segmenting the IoT devices from the manufacturing control systems. By segmenting the IoT devices from the primary manufacturing control systems, BetaTech ensures that a compromise of the IoT devices doesn't immediately put the control systems at risk. Segmentation acts as a barrier to restrict the potential spread of malicious activity.

Option A is incorrect. While a robust firewall is crucial for network security, it does not replace the need for segmentation, especially with varied devices and risk profiles.

Option B is incorrect. Although periodic password changes can enhance the security of IoT devices, it does not prevent a compromised IoT device from affecting other parts of the network.

Option D is incorrect. Automatic updates can fix known vulnerabilities in IoT devices, but they don't provide the isolation that segmentation offers to prevent a compromise from affecting other network segments.

Question 220. A software company is developing a new cloud-based application where clients can store and manage their

customer contact details. The stored data does not include financial or medical information but does contain phone numbers and email addresses. How should this information be classified?

- (A) Public
- (B) Restricted
- (C) **Sensitive**
- (D) Classified

Explanation 220. Correct Answer: C. Sensitive. Phone numbers and email addresses are considered Personally Identifiable Information (PII) and should be classified as sensitive since unauthorized access could lead to privacy violations or misuse.

Option A is incorrect. Public classification is for data that is intended for general access and holds no confidential information.

Option B is incorrect. Restricted typically applies to data that is more confidential than sensitive data, such as financial or strategic data.

Option D is incorrect. Classified is a more general term and can encompass various levels of data classification, including Top Secret, Secret, or Confidential, typically used in government sectors.

Question 221. A multinational company wants to allow its remote employees to securely access the corporate intranet over the Internet. The company's primary concern is to ensure data

confidentiality and integrity during transit. Which solution should the company implement?

- (A) VLAN
- (B) VPN
- (C) NAC
- (D) DMZ

Explanation 221. Correct Answer: B. VPN. A Virtual Private Network (VPN) allows remote users to establish a secure connection to an organization's internal network over the public internet. It encrypts the data in transit, ensuring both confidentiality and integrity.

Option A is incorrect. A VLAN (Virtual Local Area Network) is used to segment network traffic within a local network, but it does not provide encryption or a method for secure remote access.

Option C is incorrect. NAC (Network Access Control) is a security solution that enforces policy on devices attempting to access network resources, but it doesn't inherently provide encrypted communication over the internet.

Option D is incorrect. DMZ (Demilitarized Zone) is a network segment that acts as a buffer between an organization's internal network and untrusted external networks. It doesn't provide encrypted communication for remote users.

Question 222. A financial firm outsources its payment processing to a third-party service provider. After a series of fraudulent transactions, it was discovered that the service

provider was not employing the latest encryption standards when transmitting data. Which vulnerability related to supply chain does this scenario highlight?

- (A) Inadequate vendor background checks
- (B) **Service provider's outdated security practices**
- (C) Deficient hardware components from a supplier
- (D) Software with embedded backdoors

Explanation 222. Correct Answer: B. Service provider's outdated security practices. Supply chain vulnerabilities encompass risks originating from third-party vendors and service providers. In this scenario, the third-party service provider's failure to use current encryption standards for transmitting data exemplifies a vulnerability that arises due to outdated security practices by the service provider.

Option A is incorrect. While vendor background checks are essential, the scenario does not specifically point towards a problem with the vendor's background. It focuses on their encryption practices.

Option C is incorrect. The scenario doesn't mention hardware components or any issues related to them.

Option D is incorrect. The issue here pertains to encryption standards, not to software with embedded backdoors.

Question 223. A popular online shopping platform noticed that some product reviews contained a strange link which, when clicked, led users to a site that resembled the platform but harvested login credentials. What vulnerability in the review

system might have allowed attackers to post such links?

- (A) Session Hijacking
- (B) **Cross-site scripting (XSS)**
- (C) Password Spraying
- (D) Credential Stuffing

Explanation 223. Correct Answer: B. Cross-site scripting (XSS). XSS vulnerabilities allow attackers to inject malicious scripts into web content. If the platform's review system does not properly sanitize input, it could permit attackers to embed malicious links that lead to phishing sites.

Cross-site scripting attacks exploit vulnerabilities in web applications to insert malicious scripts. In this case, the ability to post malicious links within product reviews is an indication of an XSS vulnerability. When unsuspecting users click on these links, they are redirected to phishing sites designed to steal their credentials.

Option A is incorrect. Session Hijacking involves taking over an active user session. It doesn't involve posting malicious links in website content.

Option C is incorrect. Password Spraying involves attempting to authenticate against many user accounts with a few commonly used passwords. It doesn't involve embedding malicious links in website content.

Option D is incorrect. Credential Stuffing attacks involve automated attempts to gain access using large sets of valid

usernames and passwords. It isn't related to the insertion of malicious links in web content.

Question 224. An organization has decided to focus on securing its database servers where customer details and transaction records are stored. This data is not being actively accessed or processed. Which type of security measure would be MOST appropriate for this type of data?

- (A) VLDData Loss Prevention (DLP) for emailAN
- (B) Web Application Firewall (WAF)
- (C) **Full Disk Encryption (FDE)**
- (D) Intrusion Detection System (IDS) for network traffic

Explanation 224. Correct Answer: C. Full Disk Encryption (FDE). Data at rest refers to data that is not actively moving through the network, such as data stored on hard drives. Full Disk Encryption (FDE) is a security measure specifically designed to protect data at rest by encrypting the entire hard drive.

Option A is incorrect. DLP for email primarily focuses on preventing unauthorized data transfers via email and is more suited for data in transit rather than data at rest.

Option B is incorrect. WAF protects web applications from various online threats and is not specifically tailored to protect data at rest.

Option D is incorrect. An IDS for network traffic mainly focuses on monitoring and detecting malicious activity in

network traffic, which pertains to data in transit and not data at rest.

Question 225. XYZ Corp. has recently developed a new manufacturing process that reduces production costs by 50%. This process is not yet patented and is considered a trade secret. The company wants to ensure that employees do not disclose this process to competitors. Which of the following would be the MOST effective strategy to achieve this?

- (A) Providing employees with a bonus for keeping the process confidential
- (B) Conducting random checks of employee communications
- (C) **Implementing a mandatory non-disclosure agreement (NDA) for all employees**
- (D) Hosting quarterly seminars to educate employees about the value of the trade secret

Explanation 225. Correct Answer: C. Implementing a mandatory non-disclosure agreement (NDA) for all employees. An NDA is a legally binding contract that prohibits employees from disclosing confidential information, like trade secrets. If an employee breaches the NDA, the company has legal grounds to seek damages or other remedies.

Option A is incorrect. While bonuses might provide an incentive for employees, it doesn't provide a binding legal framework to protect the trade secret.

Option B is incorrect. Random checks can deter some employees but might not be effective across the board and could also lead to trust issues within the organization.

Option D is incorrect. While education is essential and can instill a sense of responsibility, it doesn't provide a legal means to protect the trade secret as an NDA does.

Question 226. While analyzing a vulnerability in a company's web application, the security team refers to a specific CVE to understand the vulnerability's details. They further assess its CVSS score to decide on the remediation urgency. Which of the following best describes the purpose of the CVE and CVSS in this context?

- (A) CVE provides a severity score, while CVSS gives a unique identifier for the vulnerability
- (B) CVE and CVSS both offer a scoring mechanism to rank vulnerabilities
- (C) **CVE provides a unique identifier, while CVSS offers a standardized severity score**
- (D) CVE and CVSS are regulatory requirements for all software applications

Explanation 226. Correct Answer: C. CVE provides a unique identifier, while CVSS offers a standardized severity score. CVE (Common Vulnerabilities and Exposures) offers a standardized identifier for vulnerabilities, ensuring clear communication and reference. CVSS (Common Vulnerability Scoring System) provides a standardized method for rating the severity of vulnerabilities, enabling organizations to prioritize remediation.

Option A is incorrect. It's the opposite. CVE gives a unique identifier, while CVSS provides a severity score.

Option B is incorrect. Only CVSS offers a scoring mechanism to rank vulnerabilities. CVE offers unique identifiers.

Option D is incorrect. While using CVE and CVSS can be considered best practices, they aren't regulatory requirements for all software applications.

Question 227. During a security assessment, Maria, a security consultant, identifies a self-signed certificate being used on a client's public-facing web server. What is the PRIMARY security concern related to this finding?

- (A) The web server might be vulnerable to Distributed Denial of Service (DDoS) attacks
- (B) The certificate could be expired
- (C) **Users cannot validate the authenticity of the website easily**
- (D) The web server might not support modern encryption algorithms

Explanation 227. Correct Answer: C. Users cannot validate the authenticity of the website easily. Self-signed certificates are not signed by a recognized Certificate Authority. As a result, when users connect to a website using a self-signed certificate, they typically receive a warning that the certificate is not trusted. This poses a risk as users cannot easily validate the authenticity of the website, making them more susceptible to man-in-the-middle attacks.

Option A is incorrect. While DDoS attacks are a concern for public-facing web servers, they aren't directly related to the use of self-signed certificates.

Option B is incorrect. Any certificate, whether self-signed or CA-signed, can expire. However, expiration is not the primary concern related to the use of self-signed certificates on public-facing servers.

Option D is incorrect. The use of modern encryption algorithms is independent of whether a certificate is self-signed or not.

Question 228. Julia, a security administrator, is concerned about potential unauthorized access to confidential project files stored on a company server. She decides to place a document within the project folders that seems enticing but is actually monitored for access. This strategy aims to detect if someone is accessing files without authorization. What is this document commonly known as?

- (A) Salt file
- (B) **Honeyfile**
- (C) Log file
- (D) Backup file

Explanation 228. Correct Answer: B. Honeyfile. A honeyfile is a monitored file placed intentionally to act as a decoy. If accessed, it can provide an alert that someone might be accessing files without proper authorization, or it might be an indication of a potential insider threat.

Option A is incorrect. A salt is random data that is used as an additional input to a one-way function that hashes data or passwords. It isn't a decoy file.

Option C is incorrect. A log file records events in an operating system or other software to aid in troubleshooting and activity monitoring, but it isn't used as a deceptive measure.

Option D is incorrect. A backup file is a copy of a file or database that can be used for data recovery. It's not a decoy to detect unauthorized access.

Question 229. A security auditor found that a website's login form returns detailed error messages like "Incorrect column name" or "Table not found." Which type of vulnerability could attackers potentially exploit using this information?

- (A) Brute Force Attack
- (B) **Structured Query Language injection (SQLi)**
- (C) Man-in-the-Middle Attack
- (D) Session Hijacking

Explanation 229. Correct Answer: B. Structured Query Language injection (SQLi). When websites provide detailed database error messages, it can give attackers clues about the database structure, making it easier for them to craft successful SQL injection attacks.

By returning detailed database error messages, the website inadvertently provides attackers with valuable insights into the database structure and potential points of vulnerability. This can

be used to refine and enhance SQLi attacks, enabling attackers to potentially access, modify, or delete data.

Option A is incorrect. A Brute Force Attack involves trying many passwords or passphrases to guess the right one. Detailed error messages from a database are not typically used in brute force attacks.

Option C is incorrect. Man-in-the-Middle Attack intercepts and possibly alters the communication between two parties. Database error messages are not directly related to this type of attack.

Option D is incorrect. Session Hijacking involves taking over an active user session. Detailed database error messages don't play a direct role in this type of attack.

Question 230. A law firm is transitioning to a digital storage system and wants to ensure that client records and case files are protected from unauthorized access. Which of the following would be the BEST strategy to ensure the confidentiality of legal information stored digitally?

- (A) Conducting regular penetration testing on the digital storage system
- (B) **Encrypting the client records and case files**
- (C) Applying watermarks to digital documents
- (D) Limiting physical access to the server room

Explanation 230. Correct Answer: B. Encrypting the client records and case files. Encryption is the process of converting information into an unreadable format unless one has the

appropriate decryption key. By encrypting legal documents, unauthorized individuals, even if they gain access to the storage system, won't be able to comprehend the content of the documents.

Option A is incorrect. While regular penetration testing is essential to identify vulnerabilities in a system, it does not directly protect the confidentiality of stored legal information.

Option C is incorrect. Watermarking documents can deter copying or unauthorized distribution, but it doesn't prevent unauthorized access or reading of the documents.

Option D is incorrect. Limiting physical access to the server room can prevent unauthorized physical access, but it does not safeguard against digital breaches or protect the content of the files.

Question 231. While conducting a routine security review, Jake, a security specialist, discovers an unexpected piece of data placed in the organization's financial system. Upon asking, he learns that this piece of data is intentionally placed and monitored to see if any unauthorized user or system interacts with it. What is this deceptive piece of data known as?

- (A) Honeystring
- (B) **Honeytoken**
- (C) Canary token
- (D) Security marker

Explanation 231. Correct Answer: B. Honeytoken.

Honeytokens are strategically placed deceptive pieces of data

that have no actual value or real-world use but are closely monitored. Their sole purpose is to detect unauthorized interactions, as any access or use of a honeypot is likely malicious or unauthorized.

Option A is incorrect. There isn't a commonly recognized security term known as "Honeystring" in the context described.

Option C is incorrect. Canary tokens are a specific type of honeypot and can serve the same purpose. However, given the choices provided and the context of the question, "Honeytoken" is the most accurate answer.

Option D is incorrect. A security marker, in a general sense, can be any mark or indicator used for security purposes, but it isn't specifically a deceptive piece of data placed to detect unauthorized access.

Question 232. You are a security consultant for a company that uses a cloud-based infrastructure. During a security review, you discover that there are no boundaries defined between the company's development, testing, and production environments in the cloud. This can lead to unintended interactions and data leaks. What kind of vulnerability is this scenario illustrating?

- (A) Insecure API endpoints
- (B) Weak encryption methods
- (C) **Lack of resource isolation**
- (D) Insufficient backup strategies

Explanation 232. Correct Answer: C. Lack of resource isolation. Cloud-specific vulnerabilities can arise due to the

shared nature of the cloud infrastructure. In this scenario, not having boundaries or isolation between different environments like development, testing, and production can lead to vulnerabilities. If there is no proper resource isolation, malicious code introduced in the development environment could make its way to production or confidential production data might be exposed in testing, leading to potential data breaches.

Option A is incorrect. Insecure API endpoints would pertain to vulnerabilities where APIs used to manage and interact with cloud services are not properly secured.

Option B is incorrect. Weak encryption methods refer to the use of outdated or vulnerable encryption algorithms, which would not directly relate to the mixing of environments.

Option D is incorrect. Insufficient backup strategies would relate to not having adequate data backup and recovery mechanisms, which is a different concern from resource isolation.

Question 233. AlphaCorp is in the final stages of selecting a cybersecurity consultant. One of the shortlisted firms, SecureWorld, recently hired AlphaCorp's former CISO as a senior consultant. Given this situation, what should be AlphaCorp's immediate concern during vendor selection?

- (A) The expertise the former CISO brings to SecureWorld
- (B) The possibility that SecureWorld could offer a discounted price

- (C) **Potential conflict of interest due to prior associations**
- (D) SecureWorld's global presence and reputation

Explanation 233. Correct Answer: C. Potential conflict of interest due to prior associations. Having the former CISO of AlphaCorp in a senior role at SecureWorld might raise concerns about potential conflicts of interest. It's essential to ensure that decisions are made objectively, and there's no bias due to prior associations.

Option A is incorrect. While the expertise of the former CISO is valuable, it's not the primary concern in this context of potential conflict of interest.

Option B is incorrect. Pricing and discounts are not the primary concern related to potential conflicts of interest in vendor selection.

Option D is incorrect. While global presence and reputation are essential factors for vendor selection, they do not directly address the issue of potential conflict of interest arising from the former CISO's position.

Question 234. An IT technician is performing a routine security audit of a company's server room. She discovers a server with outdated firmware that hasn't been updated for two years. What potential vulnerability does the outdated firmware expose the server to?

- (A) SQL Injection
- (B) Physical tampering

- (C) Unpatched exploits
- (D) Credential stuffing

Explanation 234. Correct Answer: C. Unpatched exploits.

Firmware, like software, receives updates to fix known vulnerabilities. If firmware is outdated, it can leave systems susceptible to known vulnerabilities that attackers can exploit.

Firmware serves as the foundational software for hardware devices. When firmware is not updated regularly, it may contain vulnerabilities that were patched in later versions. These vulnerabilities can potentially be exploited by attackers, putting the device and connected systems at risk.

Option A is incorrect. SQL Injection is a vulnerability associated with databases and web applications, not firmware.

Option B is incorrect. Physical tampering pertains to someone physically accessing and altering a device. While firmware vulnerabilities can sometimes lead to physical tampering (through boot-level attacks), the direct link between outdated firmware and physical tampering is not as strong as the link to unpatched exploits.

Option D is incorrect. Credential stuffing is an attack method that involves using known username-password pairs to gain unauthorized access. It isn't directly related to firmware vulnerabilities.

Question 235. As part of the company's vulnerability management initiative, the security team has decided to conduct

a series of penetration tests. Which of the following is the PRIMARY reason for incorporating penetration testing as a threat identification method?

- (A) To ensure compliance with regulatory requirements
- (B) To validate the efficiency of security awareness training
- (C) **To actively exploit vulnerabilities and assess potential impact**
- (D) To identify misconfigurations in the SIEM system

Explanation 235. Correct Answer: C. To actively exploit vulnerabilities and assess potential impact. Penetration testing is a method used to actively exploit vulnerabilities in an environment. Its primary purpose is to determine the potential impact and risk of those vulnerabilities in a real-world scenario, thereby allowing the organization to understand and prioritize remediation efforts.

Option A is incorrect. While some regulations might require penetration testing, the primary goal of the test is not just for compliance but to understand vulnerabilities' potential impact.

Option B is incorrect. Although penetration testing can sometimes be used to gauge the effectiveness of security training (for instance, in social engineering tests), it's not the primary reason for conducting these tests.

Option D is incorrect. SIEM systems are used for logging and event management. While a pen test might uncover misconfigurations in various systems, its primary purpose is not to focus on the SIEM.

Question 236. Globex Industries is expanding its data centers across multiple geographic locations. The IT team wants to have a centralized system to get real-time status, outages, and metrics of all data center infrastructures. Which of the following solutions would be the MOST effective for this purpose?

- (A) Data Loss Prevention (DLP) tools
- (B) Distributed Denial of Service (DDoS) protection
- (C) Security Information and Event Management (SIEM)
- (D) **Infrastructure Management Platform (IMP)**

Explanation 236. Correct Answer: D. Infrastructure Management Platform (IMP). IMPs provide centralized control and monitoring for infrastructure across multiple sites. They deliver insights into infrastructure health, outages, and metrics, ensuring that the IT team can address issues promptly.

Option A is incorrect. DLP tools focus on preventing unauthorized data transfers and exfiltrations, not on monitoring infrastructure health and status.

Option B is incorrect. DDoS protection tools safeguard against denial-of-service attacks but aren't designed to monitor the overall health or metrics of data center infrastructures.

Option C is incorrect. While SIEM solutions centralize log data and provide insights into security events, they are not designed primarily to monitor data center infrastructure health across multiple locations.

Question 237. After undergoing a major infrastructure upgrade, GlobalMed Corp experienced several unanticipated security

issues. In retrospect, the IT manager realized they skipped an essential step in their change management process which could have predicted and mitigated these issues. What step did they most likely overlook?

- (A) Procurement of new hardware
- (B) Training of IT staff on the new systems
- (C) **Impact analysis**
- (D) Integration with legacy systems

Explanation 237. Correct Answer: C. Impact analysis. An impact analysis is vital in the change management process as it evaluates the potential ramifications of a proposed change. By conducting this analysis, organizations can anticipate potential security challenges and mitigate them before implementing the change.

Option A is incorrect. While procurement is essential, merely purchasing new hardware wouldn't directly help in predicting or mitigating potential security issues stemming from an infrastructure upgrade.

Option B is incorrect. Training IT staff is essential for effective implementation and operation, but it doesn't directly address predicting and understanding potential security consequences of the upgrade.

Option D is incorrect. Integration with legacy systems is a crucial consideration, especially for compatibility. However, the focus of the scenario is on predicting and understanding potential security issues, which is primarily addressed through an impact analysis.

Question 238. Sarah, a software developer at a tech company, decided to gain root access to her company-issued mobile device to customize its features. Soon after, the IT department detected unauthorized data transmissions from her device. Which mobile vulnerability is most likely associated with her actions?

- (A) Side loading of applications
- (B) Inconsistent OS updates
- (C) **Mobile device jailbreaking**
- (D) Use of open Wi-Fi networks

Explanation 238. Correct Answer: C. Mobile device jailbreaking. Jailbreaking is the process of removing the restrictions imposed by the manufacturer on certain devices, thereby allowing root access. With this root access, users can install and customize software that hasn't been approved by the device's manufacturer or carrier. However, jailbreaking can expose the device to various security vulnerabilities, as indicated by unauthorized data transmissions.

Option A is incorrect. Side loading refers to the installation of applications from sources other than the official app store. While side loading can pose security risks, Sarah's actions specifically relate to gaining root access, which points to jailbreaking.

Option B is incorrect. Inconsistent OS updates refer to the presence of various versions of an OS across different devices. Sarah's actions are related to obtaining root access, not inconsistent updates.

Option D is incorrect. Using open Wi-Fi networks can expose mobile devices to threats, but Sarah's vulnerability arose from gaining root access, not from her choice of Wi-Fi networks.

Question 239. Jenna, a web administrator for a growing online retail business, is in the process of obtaining SSL certificates for the company's domain. The company uses several subdomains for different services, such as shop.example.com, blog.example.com, and support.example.com. Instead of obtaining individual certificates for each subdomain, Jenna wants to use one certificate. What type of certificate should Jenna pursue?

- (A) Extended Validation Certificate
- (B) **Wildcard Certificate**
- (C) Certificate with Subject Alternative Names (SAN)
- (D) Code Signing Certificate

Explanation 239. Correct Answer: B. Wildcard Certificate.

A Wildcard Certificate is designed to secure a domain and its subdomains under the same top-level domain. For example, a wildcard certificate for *.example.com would secure shop.example.com, blog.example.com, and any other subdomain of example.com.

Option A is incorrect. An Extended Validation Certificate provides the highest level of validation but does not necessarily cover multiple subdomains by default.

Option C is incorrect. While a Certificate with Subject Alternative Names (SAN) can secure multiple domains and

subdomains, it is not specifically tailored for all subdomains under a single domain as the Wildcard Certificate is.

Option D is incorrect. A Code Signing Certificate is used to sign software code, ensuring its integrity and authenticity, not for securing domains or subdomains.

Question 240. CyberLock Inc. is assessing the security postures of its third-party vendors to determine potential risks. The cybersecurity team wants to gather foundational security information from each vendor to evaluate their security maturity and practices. What would be the most cost-effective and efficient way to collect this data from a large number of vendors?

- (A) Conduct a penetration test for each vendor
- (B) **Send out security questionnaires to each vendor**
- (C) Visit each vendor's site for an in-person assessment
- (D) Review the annual financial reports of each vendor

Explanation 240. Correct Answer: B. Send out security questionnaires to each vendor. Security questionnaires are commonly used to gather foundational security information from third-party vendors. They are cost-effective and can efficiently collect standardized data from a large number of vendors to evaluate their security posture and practices.

Option A is incorrect. Conducting a penetration test for each vendor would be resource-intensive, costly, and may not provide the foundational information about the vendor's security practices.

Option C is incorrect. Visiting each vendor's site for an in-person assessment would be time-consuming, costly, and logistically challenging, especially when dealing with a large number of vendors.

Option D is incorrect. Annual financial reports provide financial data and do not offer in-depth details on a vendor's security posture or practices.

Question 241. A developer has implemented a new feature on a company's website that allows users to search for products by their names. Within a few days, the IT team noticed abnormal activities where entire tables from the database were being dumped. Which vulnerability might the new feature have introduced?

- (A) Cross-Site Scripting (XSS)
- (B) Distributed Denial-of-Service (DDoS)
- (C) **Structured Query Language injection (SQLi)**
- (D) Cross-Site Request Forgery (CSRF)

Explanation 241. Correct Answer: C. Structured Query Language injection (SQLi). SQLi attacks occur when an attacker can insert or "inject" SQL code into a query. If user input is not properly sanitized before being used in SQL statements, attackers can exploit this to manipulate the queries, which can lead to unauthorized viewing of data, corrupting or deleting data, and other malicious activities.

Structured Query Language injection, or SQLi, is a code injection technique that attackers use to run malicious SQL statements on a database. Given that entire tables from the

database were dumped after implementing a search feature, it's a clear indication that the feature did not properly sanitize user input, allowing for SQLi.

Option A is incorrect. Cross-Site Scripting (XSS) attacks inject malicious scripts into web pages viewed by users. It doesn't lead to dumping of database tables as described in the scenario.

Option B is incorrect. Distributed Denial-of-Service (DDoS) attacks overwhelm a target with traffic, causing service interruptions. It's not related to the extraction of database information.

Option D is incorrect. Cross-Site Request Forgery (CSRF) tricks victims into submitting malicious requests. It doesn't result in the dumping of database tables.

Question 242. DeltaSoft has released a new web application. The security team is tasked with observing the application's behavior and responses when it is running to identify potential vulnerabilities. Which method is most appropriate for this purpose?

- (A) Static Analysis
- (B) Fuzz Testing
- (C) Whitebox Testing
- (D) **Dynamic Analysis**

Explanation 242. Correct Answer: D. Dynamic Analysis.

Dynamic analysis focuses on examining an application during its execution, or runtime. By observing the application's

behavior and responses, security teams can identify vulnerabilities that might not be evident in the static code.

Option A is incorrect. Static analysis evaluates an application's code without executing the application. It does not focus on observing the application's behavior during runtime.

Option B is incorrect. Fuzz testing involves submitting random inputs to an application to observe its behavior and detect vulnerabilities, but it's just one subset of dynamic analysis.

Option C is incorrect. Whitebox testing involves understanding the internal structures and workings of an application while testing, which can be part of static or dynamic testing, but on its own, it does not specifically focus on runtime behavior observation.

Question 243. GlobalTech, a multinational corporation, is negotiating a cloud storage contract with CloudCorp. GlobalTech wants to ensure that data retrieval times remain under 2 seconds 99.9% of the time. Which component should be explicitly defined in their agreement to set this expectation?

- (A) Pricing model
- (B) Data sovereignty clauses
- (C) **Service-level agreement (SLA)**
- (D) Termination clauses

Explanation 243. Correct Answer: C. Service-level agreement (SLA). Service-level agreements (SLAs) are designed to define specific metrics, responsibilities, and expectations to ensure that both parties understand and agree to

the performance benchmarks and consequences if those benchmarks are not achieved. In this scenario, the SLA would specify the expected data retrieval times.

Option A is incorrect. While pricing is an essential aspect of any contract, it does not specify performance expectations like data retrieval times.

Option B is incorrect. Data sovereignty clauses pertain to the legal aspects of where data is stored and processed, not to performance metrics.

Option D is incorrect. Termination clauses deal with the conditions under which the agreement might be terminated, not with performance expectations.

Question 244. SoftTech Inc., a software company, is considering expanding its operations to Europe. They will be collecting and processing personal data of EU citizens. Which of the following legal implications is MOST critical for SoftTech Inc. to consider?

- (A) The need to register with each country's software association
- (B) **Compliance with the General Data Protection Regulation (GDPR)**
- (C) Ensuring software patent rights in each European country
- (D) The European standard for software coding

Explanation 244. Correct Answer: B. Compliance with the General Data Protection Regulation (GDPR). When dealing

with personal data of EU citizens, companies must comply with the GDPR, which outlines strict requirements on data protection and privacy. Non-compliance can lead to hefty fines and legal repercussions.

Option A is incorrect. Registering with each country's software association is not related to the privacy and legal implications of processing personal data.

Option C is incorrect. While software patent rights are essential, they don't directly address the privacy concerns of processing personal data of EU citizens.

Option D is incorrect. There is no "European standard for software coding" that relates to the privacy of personal data. The critical concern is data protection and privacy regulations like the GDPR.

Question 245. A multinational organization recently experienced a significant security breach. After investigating, it was determined that a change to the network infrastructure was made without undergoing the standard approval process. As a result, there was a misconfiguration which allowed unauthorized access. What security principle related to change management did the organization neglect?

- (A) Configuration baseline reviews
- (B) **Least privilege enforcement**
- (C) Approval process adherence
- (D) Patch management

Explanation 245. Correct Answer: C. Approval process

adherence. The approval process is a critical aspect of change management. Before any changes are made, especially to critical systems like network infrastructure, they need to undergo a rigorous approval process. This ensures that multiple experts evaluate the change for potential vulnerabilities or issues. In this scenario, skipping the approval process led to a significant security breach.

Option A is incorrect. Configuration baseline reviews involve regularly checking and ensuring that systems are configured as per the organization's approved baseline. While it's important, the issue in the scenario was directly related to bypassing the approval process.

Option B is incorrect. Least privilege enforcement means providing only the minimal necessary access to users to perform their tasks. This scenario doesn't deal with access rights or privileges.

Option D is incorrect. Patch management concerns the process of applying updates to software and systems. The breach in the question wasn't related to missing patches but was due to bypassing the approval process.

Question 246. Carlos, an IT consultant, advises a startup company on cybersecurity best practices. The company plans to launch several microsites under various subdomains. They want a solution that is cost-effective but also ensures that the sites are validated by a third-party. What type of certificate should Carlos recommend?

- (A) A separate self-signed certificate for each microsite
- (B) An individual third-party certificate for each subdomain
- (C) **A third-party wildcard certificate**
- (D) An EV certificate issued by an internal CA

Explanation 246. Correct Answer: C. A third-party wildcard certificate. A third-party wildcard certificate allows an organization to secure multiple subdomains with a single certificate. It's cost-effective as the company doesn't need to purchase and manage separate certificates for each subdomain, and because it's issued by a third-party Certificate Authority, it provides validation for external users.

Option A is incorrect. Self-signed certificates won't provide third-party validation, which could result in trust issues for external users.

Option B is incorrect. While individual third-party certificates for each subdomain will provide third-party validation, this approach would not be as cost-effective as a wildcard certificate.

Option D is incorrect. An EV certificate provides high assurance, but one issued by an internal CA will not be inherently trusted by external users.

Question 247. Two university research departments, UniAlpha and UniBeta, decide to collaborate on a project exploring quantum computing's security implications. They need an agreement to express mutual intentions without enforcing legally binding obligations. Which document is most suitable

for their needs?

- (A) Service-level agreement (SLA)
- (B) Non-disclosure agreement (NDA)
- (C) **Memorandum of understanding (MOU)**
- (D) Licensing agreement

Explanation 247. Correct Answer: C. Memorandum of understanding (MOU). A Memorandum of Understanding (MOU) serves as a formal agreement between parties to signal mutual intentions without necessarily introducing legally binding terms. Given that UniAlpha and UniBeta want to signify their shared intentions on a collaborative research project, an MOU is the most appropriate choice.

Option A is incorrect. An SLA is typically between a service provider and a customer and details the level of service expected.

Option B is incorrect. An NDA focuses on the confidentiality of information shared between parties.

Option D is incorrect. A licensing agreement concerns the rights to use, distribute, or reproduce software or intellectual property.

Question 248. A system administrator notices that an unauthorized user was able to obtain elevated privileges on a server, even though the default account settings were configured correctly. Upon investigation, it was found that the server's operating system had not been updated for several months. What type of vulnerability was likely exploited?

- (A) Application Misconfiguration
- (B) **OS Patch Management Issue**
- (C) Weak Encryption Algorithm
- (D) Password Reuse Attack

Explanation 248. Correct Answer: B. OS Patch

Management Issue. When operating systems are not regularly updated, they become vulnerable to known exploits that have since been patched by vendors. An attacker can take advantage of these vulnerabilities to gain unauthorized elevated privileges.

Operating system-based vulnerabilities often arise due to missed patches or updates. Keeping the OS updated is crucial because vendors frequently release patches to address known vulnerabilities. In this case, the lapse in updating the operating system opened a window for attackers to exploit and obtain elevated privileges.

Option A is incorrect. Application Misconfiguration pertains to incorrect settings or configurations in software applications, not operating systems. The scenario does not suggest any issues with application settings.

Option C is incorrect. Weak Encryption Algorithm refers to encryption that can be easily decrypted or broken due to flaws in the algorithm itself. The scenario doesn't mention encryption or decryption problems.

Option D is incorrect. Password Reuse Attack involves an attacker using previously breached passwords to access

different accounts. The scenario doesn't indicate password-related issues.

Question 249. Jane, an accountant in a multinational corporation, received an email from what seemed to be the company's IT department. The email had the company's logo, colors, and font and urged Jane to click on a link to reset her password due to "suspicious activity." However, upon close inspection, Jane noticed a minor spelling error in the domain name of the sender's email address. What type of attack does this scenario describe?

- (A) Spear Phishing
- (B) Vishing
- (C) Baiting
- (D) **Brand Impersonation**

Explanation 249. Correct Answer: D. Brand Impersonation.

The attacker has mimicked the company's branding in an attempt to deceive the recipient into thinking the communication is legitimate.

Brand impersonation involves attackers mimicking or replicating the branding of a reputable company or organization in an attempt to trick users into thinking the communication is legitimate. This tactic is commonly used in phishing emails to mislead recipients into providing sensitive information or clicking on malicious links.

Option A is incorrect. Spear Phishing is targeted phishing aimed specifically at one individual or a small group. While Jane might be specifically targeted, the defining feature of this

attack is the impersonation of the company's branding, making it brand impersonation.

Option B is incorrect. Vishing involves voice communication or phone calls, and the scenario describes an email-based attack.

Option C is incorrect. Baiting typically offers something enticing to lure victims. There's no offer or lure in the described scenario.

Question 250. As the Chief Security Officer (CSO) of AlphaTech, you are in the process of finalizing a partnership agreement with a third-party provider. To ensure ongoing security compliance and transparency, you want to reserve the right for your organization to inspect the vendor's operations and security measures in the future. Which clause should you ensure is included in the contract?

- (A) Non-disclosure agreement (NDA)
- (B) Service level agreement (SLA)
- (C) Termination clause
- (D) **Right-to-audit clause**

Explanation 250. Correct Answer: D. Right-to-audit clause. The right-to-audit clause allows an organization to review or audit a vendor's procedures, systems, records, and practices to ensure they comply with agreed-upon security and privacy requirements.

Option A is incorrect. While an NDA is essential to protect confidential information, it doesn't give an organization the right to audit a vendor's practices.

Option B is incorrect. An SLA sets expectations around the quality and availability of services provided, but it doesn't pertain to the right to audit.

Option C is incorrect. A termination clause defines the conditions under which a partnership can be ended, but it doesn't grant audit rights.

Question 251. After a major security incident, DeltaTech implemented several security patches to address vulnerabilities in their infrastructure. To ensure the effectiveness of these patches, what should be DeltaTech's primary next step?

- (A) Deploy additional firewalls at the network perimeter
- (B) Provide cybersecurity training to all employees
- (C) **Rescan the systems to check if vulnerabilities are effectively addressed**
- (D) Change all user passwords across the organization

Explanation 251. Correct Answer: C. Rescan the systems to check if vulnerabilities are effectively addressed. After implementing security patches, it's essential to rescan the systems to ensure that the identified vulnerabilities have been effectively addressed and the patches have been implemented correctly.

Option A is incorrect. While firewalls are crucial for security, deploying them is not directly related to validating the effectiveness of newly implemented patches.

Option B is incorrect. Cybersecurity training for employees is vital, but it doesn't directly validate the success of the applied patches.

Option D is incorrect. Changing user passwords can be a necessary step after a breach, but it doesn't validate if the patches have successfully addressed vulnerabilities.

Question 252. A Security Analyst at BetaTech is reviewing the monitoring tools deployed across the organization. She wants to ensure that every tool can detect unauthorized changes made to system files and configurations. Which of the following tools is BEST suited for this purpose?

- (A) Network protocol analyzer
- (B) **File integrity monitoring (FIM) system**
- (C) Bandwidth monitoring tool
- (D) Passive vulnerability scanner

Explanation 252. Correct Answer: B. File integrity monitoring (FIM) system. File integrity monitoring systems are designed to detect and alert when unauthorized changes are made to system files and configurations, ensuring the integrity of these critical components.

Option A is incorrect. While network protocol analyzers can capture and analyze network traffic, they are not specifically designed to monitor changes to system files and configurations.

Option C is incorrect. Bandwidth monitoring tools primarily track network usage and bandwidth consumption, not modifications to system files.

Option D is incorrect. Passive vulnerability scanners monitor network traffic to detect vulnerabilities but do not actively track changes to system files.

Question 253. An e-commerce company wants to ensure that their customers' credit card data remains confidential while in transit over the internet. They are seeking a protocol that can help in securing their website's communication. Which protocol would best fit this requirement?

- (A) IPsec
- (B) SSH
- (C) TLS
- (D) ICMP

Explanation 253. Correct Answer: C. TLS. Transport Layer Security (TLS) is a cryptographic protocol that ensures data confidentiality and integrity over the internet. Websites use TLS to secure all communications between their servers and web browsers, making it suitable for e-commerce platforms to secure sensitive customer data.

Option A is incorrect. IPsec is a suite of protocols that secures IP communications by encrypting and authenticating all IP packets. It is more commonly used for VPNs rather than securing web communications.

Option B is incorrect. SSH (Secure Shell) is primarily used for secure remote access to systems, not for securing web-based communications.

Option D is incorrect. ICMP (Internet Control Message Protocol) is used by network devices to send error messages and operational information, not for securing data in transit.

Question 254. After a recent security breach, Sarah, a cybersecurity analyst, is implementing additional measures to detect unauthorized activities. She decides to embed specific values in the database that serve no real purpose but are monitored for any unauthorized access or usage. These values are designed to raise alerts if they are ever accessed or used. What are these specific values commonly referred to as?

- (A) Security flags
- (B) Honeypots
- (C) **Honeytokens**
- (D) Audit trails

Explanation 254. Correct Answer: C. Restoring systems from verified backups. Restoring systems from verified backups is a corrective control, as it can restore compromised systems to their last known good state. This action corrects the adverse effects of the intrusion and ensures that any malicious alterations are removed.

Option A is incorrect. Implementing Intrusion Detection Systems (IDS) is a detective control. It monitors and detects malicious activities in the network but doesn't correct the adverse impacts of an intrusion.

Option B is incorrect. Frequently updating firewall rules is a preventive measure, aiming to block malicious traffic and

prevent potential intrusions. While vital, it doesn't correct the impacts of an already occurred breach.

Option D is incorrect. Enabling multi-factor authentication is a preventive control, aiming to provide additional layers of verification. While it enhances security, it doesn't correct the adverse impacts of an intrusion.

Question 255. Maria receives a text message on her phone from an unknown number, stating that she has won a gift card worth \$500 from a popular online store. The message includes a link asking her to click on it to claim her prize. Maria is unsure about the authenticity of the message. Which of the following is the BEST course of action for Maria?

- (A) Click the link to check if the website looks genuine
- (B) Forward the message to her friends to verify if they received a similar message
- (C) **Delete the message without clicking on any links**
- (D) Respond to the sender asking for more details about the offer

Explanation 255. Correct Answer: C. Delete the message without clicking on any links. Messages from unknown sources, especially those that sound too good to be true, often signal a potential security threat. It's safest to delete such messages without interacting with any links.

Smishing is a type of phishing attack wherein attackers use SMS to deceive users into divulging personal information, visiting a malicious website, or downloading malware onto their

smartphones. Users should always be cautious of unsolicited messages from unknown numbers.

Option A is incorrect. Clicking the link, even out of curiosity, can lead to a malicious website or download malware onto Maria's device.

Option B is incorrect. While forwarding the message to friends might give her insight into its authenticity, it could also expose her friends to potential threats if the message is malicious.

Option D is incorrect. Responding to the sender could give them more information about Maria or confirm that her number is active, leading to further targeted attacks.

Question 256. At AlphaTech, the security team is assessing vulnerabilities in a newly deployed cloud infrastructure. While analyzing potential risks, they consider factors such as the physical location of data centers, local laws and regulations, and natural disaster frequencies. What are these considerations known as in the context of vulnerability management?

- (A) Asset valuation factors
- (B) Risk response variables
- (C) Threat intelligence variables
- (D) **Environmental variables**

Explanation 256. Correct Answer: D. Environmental variables. Environmental variables in vulnerability management refer to external factors that can influence or affect the security posture of an organization. These can include

physical location, local laws and regulations, and the potential for natural disasters.

Option A is incorrect. Asset valuation factors primarily deal with determining the value of an asset to the organization and don't typically consider external factors like local laws or natural disaster frequencies.

Option B is incorrect. Risk response variables pertain to the organization's strategies and actions to respond to identified risks rather than the external factors influencing risk.

Option C is incorrect. Threat intelligence variables revolve around information regarding potential threats or threat actors. They don't typically encompass physical environment considerations like those described in the scenario.

Question 257. During an e-commerce website audit, a security analyst discovers that if a user tries to purchase a product and simultaneously cancels the order, the product sometimes gets added to the user's cart without deducting any funds. This vulnerability can potentially be exploited to obtain products for free. Which vulnerability type is the e-commerce website susceptible to?

- (A) Directory Traversal
- (B) Insecure Direct Object References (IDOR)
- (C) **Race Condition**
- (D) Cross-Site Request Forgery (CSRF)

Explanation 257. Correct Answer: C. Race Condition. When an application's unintended behavior is due to the timing of

concurrent events or operations, it indicates a race condition. Here, the simultaneous purchase and cancellation result in a faulty outcome.

A race condition occurs when an application's behavior is dependent on the order or timing of uncontrollable events. If two operations, which aren't meant to happen simultaneously, occur at the same time, it can lead to unpredictable and unintended outcomes, like the described scenario where a product is added without payment due to the concurrency of purchase and cancellation.

Option A is incorrect. Directory Traversal vulnerabilities allow attackers to access files and directories that are stored outside the intended folder. This doesn't align with the described scenario.

Option B is incorrect. Insecure Direct Object References (IDOR) vulnerabilities occur when an attacker can access resources they're not authorized for by manipulating input, such as URL or form parameters. It's unrelated to the timing or concurrency of actions.

Option D is incorrect. Cross-Site Request Forgery (CSRF) tricks the victim into submitting a malicious request. It's about unauthorized actions rather than issues arising from the timing of legitimate ones.

Question 258. XYZ Corp., a multinational company, recently underwent a security audit. The Chief Information Security Officer (CISO) needs to report the findings of the audit to the

company's internal stakeholders as well as to a governmental regulatory agency. Which of the following represents the correct type of compliance reporting for each recipient?

- (A) Internal report for the regulatory agency and external report for internal stakeholders
- (B) External report for both the regulatory agency and internal stakeholders
- (C) **Internal report for internal stakeholders and external report for the regulatory agency**
- (D) No report is required for internal stakeholders, only an external report for the regulatory agency

Explanation 258. Correct Answer: C. Internal report for internal stakeholders and external report for the regulatory agency. Internal compliance reports are typically designed for consumption within the organization and may contain details that are not shared externally. External compliance reports, on the other hand, are designed for entities outside of the organization, such as regulators or other third parties, and would contain information that is relevant and necessary for those entities to review.

Option A is incorrect. It is not standard to provide an internal report for an external entity or an external report for internal stakeholders.

Option B is incorrect. While it's conceivable to use the same report for both internal and external entities, it's more common to tailor reports to the specific audience. An internal report may contain more detailed or sensitive information not suitable for an external audience.

Option D is incorrect. It is crucial for internal stakeholders to be aware of the audit findings to make informed decisions and plan remediation actions.

Question 259. During a critical financial quarter, GlobalFin Corp experienced unexpected outages during peak business hours due to system maintenance, impacting its operations significantly. To prevent such occurrences in the future, what should GlobalFin Corp implement regarding their maintenance activities?

- (A) Conduct maintenance activities randomly to avoid predictability
- (B) Implement maintenance activities during peak business hours
- (C) **Establish designated maintenance windows**
- (D) Reduce the frequency of maintenance activities

Explanation 259. Correct Answer: C. Establish designated maintenance windows. Maintenance windows are specific time frames designated for system maintenance, ensuring that disruptions due to updates, patches, or other maintenance activities don't occur during critical business hours. By setting these windows, usually during off-peak times, businesses can minimize operational disruptions.

Option A is incorrect. Conducting maintenance activities randomly can lead to unpredictable outages, which can be disruptive to business operations and degrade trust among stakeholders.

Option B is incorrect. Implementing maintenance activities during peak business hours is precisely what led to the disruption in the scenario. This approach would likely cause more operational problems, especially for businesses with critical operations during these hours.

Option D is incorrect. Reducing the frequency of maintenance activities might decrease disruptions, but it could also lead to unpatched vulnerabilities, outdated software, or other security and operational issues.

Question 260. Alex, a new intern at an IT company, wanted to access the internal company portal. Instead of typing “companyportal.com,” he accidentally typed “comapnyportal.com” and ended up on a site that looked identical but asked him to download a security certificate. This scenario best describes which type of attack?

- (A) Spear Phishing
- (B) Watering Hole Attack
- (C) **Typosquatting**
- (D) Man-in-the-Middle

Explanation 260. Correct Answer: C. Typosquatting. The attacker relies on typographical errors made by users when inputting a URL into a web browser, then potentially tries to exploit the user in some manner on the deceptive site.

Typosquatting, also known as URL hijacking, involves attackers registering domains that are misspellings of popular websites. The intent is often to deceive users who mistype a URL, leading them to malicious websites.

Option A is incorrect. Spear Phishing targets specific individuals or companies with tailored attempts to steal information. The described scenario revolves around the exploitation of typographical errors, not a targeted email attack.

Option B is incorrect. A Watering Hole Attack involves compromising a specific website or service that the target frequently uses. It doesn't rely on typographical errors.

Option D is incorrect. A Man-in-the-Middle attack involves an attacker secretly intercepting and potentially altering communication between two parties. This is not described in the scenario.

Question 261. DataGuard Corp. operates in the European Union and has recently suffered a major data breach affecting the personal data of thousands of users. They failed to comply with some key provisions of the General Data Protection Regulation (GDPR). Which of the following is the MOST likely immediate consequence of their non-compliance?

- (A) They will be forced to shut down operations until compliance is achieved
- (B) DataGuard's executive team will face immediate imprisonment
- (C) The company will be required to issue a public apology
- (D) **DataGuard Corp. will face substantial fines for their non-compliance**

Explanation 261. Correct Answer: D. DataGuard Corp. will face substantial fines for their non-compliance. The GDPR provisions can levy hefty fines on organizations that do not

comply with its requirements, especially in the case of data breaches. The fines can be up to 4% of the annual global turnover or €20 million, whichever is higher.

Option A is incorrect. While the GDPR can impose operational restrictions, it does not directly mandate shutdowns of companies due to non-compliance.

Option B is incorrect. GDPR does not call for the imprisonment of executive teams. However, non-compliance can lead to severe fines.

Option C is incorrect. While issuing a public apology might be a good PR move, it is not a direct consequence enforced by GDPR.

Question 262. A pharmaceutical company is working on a new drug formula that promises to revolutionize the treatment of a particular disease. The R&D team has detailed documentation on the components, procedures, and results of the drug trials. How should this documentation be classified to ensure that only the right people within the company have access?

- (A) Unclassified
- (B) Public
- (C) **Confidential**
- (D) Sensitive

Explanation 262. Correct Answer: C. Confidential. This drug formula and its documentation represent valuable intellectual property for the pharmaceutical company. To protect against

theft, corporate espionage, or accidental disclosure, it should be classified as confidential to ensure limited, controlled access.

Option A is incorrect. Unclassified data doesn't require any special protection or confidentiality and is inappropriate for valuable intellectual property.

Option B is incorrect. Public classification would make the information accessible to everyone, which is not suitable for proprietary drug formulas.

Option D is incorrect. While the drug formula is sensitive information, the "Confidential" classification offers stricter controls and is more suitable for such valuable intellectual property.

Question 263. After a recent software update, a company's intranet portal has been inaccessible to a few employees. The IT team suspects it could be due to network filtering rules. What should the IT team review to confirm their suspicions?

- (A) The content filtering policies
- (B) The malware detection logs
- (C) **The allow list/deny list configurations**
- (D) The network bandwidth utilization graphs

Explanation 263. Correct Answer: C. The allow list/deny list configurations. Network accessibility issues, especially after software or configuration changes, can often arise due to misconfigured allow lists or deny lists. Reviewing these configurations can help determine if specific IP addresses or

domains have been incorrectly blocked or not allowed, causing the inaccessibility issues.

Option A is incorrect. Content filtering policies primarily focus on blocking specific types of content (like social media or adult sites) rather than causing inaccessibility to specific users or departments.

Option B is incorrect. Malware detection logs track potential security threats and not network access configurations. They wouldn't typically cause a selective inaccessibility issue unless a specific user's machine is quarantined.

Option D is incorrect. While network bandwidth utilization graphs might show reduced traffic, they won't provide details on specific allow/deny list configurations that might be causing the inaccessibility.

Question 264. MegaCorp recently introduced a new web application for its customers. Before its release, the software underwent rigorous testing in a controlled environment. When the application was deployed in production, several security vulnerabilities were reported. Which of the following reasons can explain the mismatch between the test results and actual vulnerabilities?

- (A) The testing environment was an exact replica of the production environment
- (B) **Test results were not thoroughly reviewed**
- (C) The software was not tested for zero-day vulnerabilities
- (D) Penetration testing was done post-production

Explanation 264. Correct Answer: B. Test results were not thoroughly reviewed. Even if an application is tested rigorously, it is crucial to thoroughly review and interpret the test results to identify any potential security vulnerabilities. Failing to review or misinterpreting these results can lead to vulnerabilities going unnoticed and unresolved.

Option A is incorrect. Having a testing environment that mirrors the production environment is a best practice. This ensures that the tests are representative of how the software will behave in production.

Option C is incorrect. While zero-day vulnerabilities are a concern, by definition, they are unknown vulnerabilities. Testing specifically for them would be challenging. However, thorough testing and review processes can mitigate potential risks.

Option D is incorrect. Penetration testing is an essential aspect of security testing, but doing it post-production doesn't explain the mismatch between the test results and actual vulnerabilities if the initial test results were not reviewed correctly.

Question 265. NexTech, a cloud-based software company, recently faced a security breach due to inconsistent practices among its system administrators. To avoid such inconsistencies in the future, what should NexTech emphasize in its operations?

- (A) Rely on system administrators to develop their personal methods
- (B) Mandate frequent system reboots
- (C) **Implement Standard Operating Procedures (SOPs)**

for all technical operations

(D) Conduct random security audits without notifying administrators

Explanation 265. Correct Answer: C. Implement Standard Operating Procedures (SOPs) for all technical operations.

Standard Operating Procedures (SOPs) provide a consistent and documented process that employees can follow. By implementing SOPs, businesses ensure that tasks are performed uniformly, reducing the risk of errors and inconsistencies that might lead to security vulnerabilities.

Option A is incorrect. Relying on individual system administrators to develop their personal methods can lead to inconsistent practices and operational inefficiencies, increasing the risk of security breaches.

Option B is incorrect. Frequent system reboots, while they might be part of some SOPs, don't address the root issue of inconsistency among system administrators. It's the consistent method of operations that prevents errors, not just frequent restarts.

Option D is incorrect. While security audits are essential, conducting them without notice doesn't address the core issue of inconsistency in system administration practices.

Question 266. After running a vulnerability scan on the company's infrastructure, a security analyst notices a reported vulnerability on a server. However, after manual verification, the analyst determines that the vulnerability doesn't actually

exist on the server. What is this situation best described as?

- (A) A false negative
- (B) A true positive
- (C) **A false positive**
- (D) A confirmation bias

Explanation 266. Correct Answer: C. A false positive. A false positive in vulnerability management occurs when a system incorrectly flags a threat or vulnerability that isn't truly present. This can lead to wasted resources on investigating and attempting to remediate a non-existent issue.

Option A is incorrect. A false negative would mean that the vulnerability exists, but the system failed to detect it, which is the opposite of the scenario described.

Option B is incorrect. A true positive means that the vulnerability was correctly identified and truly exists, which isn't the case here.

Option D is incorrect. Confirmation bias is a cognitive bias where one favors information that confirms their existing beliefs. It's not relevant to the scenario of incorrectly detected vulnerabilities.

Question 267. Your organization has been repeatedly ignoring the security guidelines set forth by a global standards organization, despite having pledged adherence. Given the repetitive nature of these violations, the organization is now facing disciplinary measures. Which of the following is the MOST likely immediate consequence of these actions?

- (A) Immediate revocation of business licenses
- (B) **Sanctions imposed by the global standards organization**
- (C) Forcible shutdown of all online operations for a determined period
- (D) Mandatory public apology to stakeholders

Explanation 267. Correct Answer: B. Sanctions imposed by the global standards organization. Sanctions are penalties or other means of enforcement used to provide incentives for obedience with the law, or with rules and regulations. In this scenario, the global standards organization can impose sanctions for the failure to adhere to their guidelines.

Option A is incorrect. Revocation of business licenses is typically a drastic measure and might be taken by a local or national regulatory body, not a standards organization.

Option C is incorrect. While some sanctions might involve restrictions, forcibly shutting down all online operations would be an extreme and less likely measure for non-compliance with guidelines from a standards organization.

Option D is incorrect. A public apology, while potentially useful for public relations, is not a direct consequence or sanction imposed by most standards organizations.

Question 268. Sophia, the cybersecurity lead at XYZ Corp, is in the process of drafting a new security policy. During the drafting process, she primarily consults with her security team. However, upon implementation, several departments pushed

back due to the policy interfering with their operations. Which best describes the misstep Sophia made during the policy creation process?

- (A) Not using a standardized security framework
- (B) Over-reliance on automated security solutions
- (C) **Not including key stakeholders in the policy drafting process**
- (D) Focusing too much on external threats rather than internal ones

Explanation 268. Correct Answer: C. Not including key stakeholders in the policy drafting process. Stakeholders from different departments provide crucial insights into how security measures can impact various operations and processes within an organization. By including them in the policy drafting process, Sophia would have received feedback that could have helped shape a policy that not only maintains security but also aligns with the needs of different departments.

Option A is incorrect. While using a standardized security framework can provide guidance, it doesn't necessarily account for the unique operational needs of different departments within an organization.

Option B is incorrect. The scenario doesn't mention any reliance, over or otherwise, on automated security solutions.

Option D is incorrect. While both external and internal threats are crucial considerations, the primary issue here was the lack of consultation with key stakeholders.

Question 269. A company's network administrator notices that several switches in the network infrastructure are no longer receiving firmware updates from the manufacturer. These devices are no longer sold or supported. What vulnerability do these switches introduce to the network?

- (A) Physical hardware tampering
- (B) Lack of redundancy
- (C) **Increased susceptibility to new threats**
- (D) Wireless interference

Explanation 269. Correct Answer: C. Increased susceptibility to new threats. End-of-life hardware often does not receive security updates or patches, making them more vulnerable to new and evolving threats over time.

End-of-life (EOL) hardware refers to devices that are no longer supported by their manufacturers. This lack of support means that the devices won't receive any further security updates, patches, or technical support. Consequently, these devices become more susceptible to new threats and vulnerabilities, posing a security risk to the network.

Option A is incorrect. End-of-life status doesn't inherently make a device more vulnerable to physical tampering. However, without ongoing updates, they might be susceptible to firmware or software-based attacks, which could lead to physical tampering in some scenarios.

Option B is incorrect. Lack of redundancy refers to a single point of failure in a system or network. It is not directly related to the vulnerabilities associated with EOL hardware.

Option D is incorrect. Wireless interference is related to the disruption of wireless signals and is not a direct consequence of EOL hardware.

Question 270. Liam, the CTO of a medium-sized enterprise, noticed that several software applications were not updated regularly, leading to potential security vulnerabilities. Upon investigation, he realized that no specific team or individual was assigned as the owner of these applications. To enhance security, what should Liam emphasize?

- (A) Immediate decommissioning of all unowned applications
- (B) Assignment of clear ownership to all business applications**
- (C) Conducting monthly vulnerability assessments on all applications
- (D) Outsourcing the management of these applications to third-party vendors

Explanation 270. Correct Answer: B. Assignment of clear ownership to all business applications. Assigning clear ownership ensures that there's a designated team or individual responsible for the upkeep, updates, and security of an application. When there's clear ownership, the owner has the accountability to maintain and secure the application, reducing the risk of oversights like missing updates.

Option A is incorrect. Immediate decommissioning may not be practical or feasible, especially if the applications are critical to business operations.

Option C is incorrect. While monthly vulnerability assessments can help identify security issues, they don't address the root cause of the problem highlighted in the scenario – the lack of ownership and accountability.

Option D is incorrect. Outsourcing may shift the responsibility, but it doesn't ensure that the applications will be better managed or more secure. Ownership clarity is paramount, whether the management is internal or outsourced.

Question 271. Sophia received an email from her bank asking her to urgently update her personal details due to a system upgrade. The email contains a link that redirects to a website that looks similar to her bank's website. Which of the following should she do FIRST?

- (A) Follow the link and promptly update her personal details to avoid any inconvenience
- (B) Forward the email to her friends and family to ensure they are also aware of the bank's system upgrade
- (C) Delete the email immediately without taking any action
- (D) **Contact her bank through official channels to verify the authenticity of the email**

Explanation 271. Correct Answer: D. Contact her bank through official channels to verify the authenticity of the email. Before taking action based on an unsolicited email, especially one that asks for personal information or credentials, it's essential to verify its legitimacy directly with the institution or entity it claims to represent.

Phishing attacks often use fear, urgency, or perceived authority to lure victims into providing sensitive data. The best defense against such attempts is to independently verify any unexpected or suspicious requests before taking action.

Option A is incorrect. Directly responding to a potential phishing email by providing personal details is a common mistake, making the user vulnerable to fraud and identity theft.

Option B is incorrect. Forwarding a potentially malicious email to others can further propagate the threat and possibly compromise their security as well.

Option C is incorrect. While deleting the email might prevent Sophia from falling for the phishing attempt, it's still a good practice to inform the bank about the suspicious email so they can take appropriate measures and warn other customers.

Question 272. AlphaTech, a growing SaaS company, has multiple applications deployed across different cloud providers. The security team struggles to manage and analyze logs from these disparate sources. Which solution would BEST help AlphaTech centralize their logs for a more streamlined analysis?

- (A) Network Intrusion Detection System (NIDS)
- (B) **Log Aggregation Tool**
- (C) Data Loss Prevention (DLP) software
- (D) Vulnerability Scanner

Explanation 272. Correct Answer: B. Log Aggregation Tool. Log aggregation tools are specifically designed to gather,

centralize, and manage logs from various sources, making it easier to analyze and correlate events.

Option A is incorrect. While a NIDS can help detect malicious activity on a network, it doesn't centralize logs from different application sources.

Option C is incorrect. DLP software focuses on preventing unauthorized data transfers and does not serve the purpose of centralizing logs.

Option D is incorrect. Vulnerability Scanners are designed to identify vulnerabilities in a system but don't aggregate logs from various sources.

Question 273. AlphaTech is seeking a comprehensive source of intelligence about the latest cyber threats targeting its specific industry. While OSINT provides valuable data, the company is considering investing in a more specialized solution. Which of the following would best address AlphaTech's needs?

- (A) Implementing internal honeypots to trap attackers
- (B) **Subscribing to a third-party threat intelligence feed**
- (C) Regularly attending cyber security conferences
- (D) Using open-source vulnerability scanners

Explanation 273. Correct Answer: B. Subscribing to a third-party threat intelligence feed. A third-party threat intelligence feed, especially one tailored for a specific industry, provides specialized, often real-time information about cyber threats, offering insights beyond what's available in the public domain.

Option A is incorrect. While honeypots can help understand the tactics of attackers targeting the organization, they don't provide comprehensive intelligence about industry-wide threats.

Option C is incorrect. Attending cyber security conferences can offer insights and updates, but it's not a continuous or real-time source of threat intelligence.

Option D is incorrect. Open-source vulnerability scanners help identify vulnerabilities within an organization's infrastructure but don't offer specialized intelligence about industry-specific cyber threats.

Question 274. An employee receives a call from someone claiming to be from the IT department. The caller says there's an urgent update required on the employee's computer and asks for login credentials to perform the update remotely. The employee becomes suspicious because of which red flag regarding impersonation?

- (A) The caller did not use technical jargon
- (B) **IT normally sends email notifications about updates**
- (C) The employee was not expecting any updates
- (D) The caller's voice sounded unfamiliar

Explanation 274. Correct Answer: B. IT normally sends email notifications about updates. If the organization's standard procedure is to send email notifications about updates, an unsolicited call asking for credentials would be a clear red flag.

Impersonation is a common tactic used in social engineering attacks where the attacker pretends to be someone the victim trusts. Recognizing deviations from standard procedures can help identify impersonation attempts.

Option A is incorrect. The use or lack of technical jargon isn't a reliable indicator of impersonation. Some genuine IT personnel might avoid jargon to make things clearer for non-tech-savvy employees.

Option C is incorrect. While unexpected updates can be suspicious, they aren't necessarily indicative of impersonation on their own. Legitimate unexpected updates can occur.

Option D is incorrect. An unfamiliar voice isn't a reliable indicator since large organizations might have many IT personnel that an employee hasn't interacted with.

Question 275. As a security consultant, you are hired by a multinational corporation to assess the security posture of their potential vendors. One of the vendors appears promising, but your client wants to ensure that the vendor periodically examines and strengthens its own internal procedures and security controls. What should you advise your client to request from this vendor?

- (A) The vendor's business continuity plan
- (B) A list of the vendor's clients
- (C) **Evidence of internal audits**
- (D) The vendor's company mission statement

Explanation 275. Correct Answer: C. Evidence of internal audits. Requesting evidence of internal audits would allow the client to review the vendor's commitment to maintaining and improving its internal procedures and security controls.

Option A is incorrect. While a business continuity plan is essential, it primarily outlines how disruptions will be managed and does not necessarily provide evidence of the vendor's internal control practices.

Option B is incorrect. Knowing the vendor's clients can provide some context, but it does not directly provide evidence of the vendor's internal control practices or security measures.

Option D is incorrect. The company's mission statement provides an overview of the company's goals and values but doesn't provide specific evidence of its internal control practices.

Question 276. TechDynamics, a growing tech startup, plans to scale its operations and serve a global clientele. Given that their client base operates in multiple time zones, when should TechDynamics schedule their system maintenance to ensure minimal disruption?

- (A) During the busiest hours for their headquarters' local time
- (B) Staggered based on the peak hours of their global clients
- (C) Only when a system breakdown occurs
- (D) **Establish a consistent maintenance window during off-peak hours for the majority of their clientele**

Explanation 276. Correct Answer: D. Establish a consistent maintenance window during off-peak hours for the majority of their clientele. When serving a global clientele operating in various time zones, it's crucial to establish a maintenance window during hours when the majority of clients are least active. This minimizes disruptions and ensures smooth operations for most clients.

Option A is incorrect. Focusing only on the headquarters' local time disregards the operational hours of global clients. This approach might cause disruptions for clients in other time zones.

Option B is incorrect. While staggering maintenance based on peak hours of global clients seems logical, it could lead to a complex and hard-to-manage maintenance schedule, especially as the client base grows.

Option C is incorrect. Waiting for a system breakdown to perform maintenance is reactive rather than proactive. This approach might lead to more extended and unpredictable downtimes, resulting in greater disruptions and potential security risks.

Question 277. A defense contractor is working on a new missile system. While the detailed schematics and operational details are classified, they have an overview document that only a select group of partners and stakeholders can view. How should this overview document be classified?

- (A) Public
- (B) **Restricted**

- (C) Confidential
- (D) Top Secret

Explanation 277. Correct Answer: B. Restricted.

“Restricted” classification is used when access to the document or data needs to be limited to a particular group of individuals. In this scenario, only a select group of partners and stakeholders are allowed to view the overview document, making “Restricted” the most appropriate classification.

Option A is incorrect. “Public” classification would allow anyone to access the document, which is not suitable for this scenario.

Option C is incorrect. While “Confidential” classification would provide a level of protection, it doesn’t specifically restrict access to a defined group as “Restricted” does.

Option D is incorrect. “Top Secret” is a high-level classification that would be more appropriate for the detailed schematics and operational details rather than an overview document.

Question 278. TechFusion and CodeRush, two independent software development companies, are collaborating on a project that is expected to define industry standards for a new coding language. While both parties have an understanding of shared responsibilities, they have not yet established legally binding obligations. Which type of agreement best suits their current collaborative understanding?

- (A) Service-level agreement (SLA)

- (B) Non-disclosure agreement (NDA)
- (C) **Memorandum of agreement (MOA)**
- (D) Licensing agreement

Explanation 278. Correct Answer: C. Memorandum of agreement (MOA). A Memorandum of Agreement (MOA) outlines mutual understandings and responsibilities between two or more parties and does not necessarily contain legally binding obligations. In this scenario, TechFusion and CodeRush have a shared understanding but have not reached legally binding terms, making an MOA the most appropriate choice.

Option A is incorrect. An SLA specifies performance metrics and expectations between a service provider and a customer. It doesn't necessarily suit a collaborative project aiming to define industry standards.

Option B is incorrect. An NDA pertains to the confidentiality of information and would not define mutual understandings or responsibilities related to project collaboration.

Option D is incorrect. A licensing agreement typically deals with the rights to use, distribute, or reproduce software or intellectual property.

Question 279. A security analyst at CyberSecure Corp. reviews a vulnerability report concerning an application that could allow attackers to upload malicious scripts. Once these scripts are executed, they can grant attackers complete control over the application. How should this vulnerability be primarily classified?

- (A) Integrity vulnerability
- (B) Availability vulnerability
- (C) **Remote code execution vulnerability**
- (D) Disclosure vulnerability

Explanation 279. Correct Answer: C. Remote code execution vulnerability. Remote code execution (RCE) vulnerabilities allow attackers to run arbitrary commands or scripts on a targeted system. In the scenario, the application vulnerability grants attackers the ability to upload and execute malicious scripts, which aligns with this classification.

Option A is incorrect. While the vulnerability can affect the integrity of the application, the primary concern here is the ability of attackers to execute code remotely, making it an RCE vulnerability.

Option B is incorrect. Availability vulnerabilities primarily concern the disruption of services or systems, preventing authorized users from accessing them. The scenario doesn't indicate any disruption of availability.

Option D is incorrect. Disclosure vulnerabilities involve unauthorized viewing or accessing of information. The described vulnerability goes beyond mere disclosure, allowing execution of malicious scripts.

Question 280. A financial institution is updating its infrastructure to ensure that customer financial data is kept secure from both internal and external threats. Which of the following would be the MOST effective measure to protect

customer financial data from being accessed by unauthorized internal users?

- (A) Deploying perimeter firewalls around the institution's network
- (B) Implementing two-factor authentication (2FA) for all customer accounts
- (C) **Enforcing strict access controls based on the principle of least privilege**
- (D) Conducting yearly cybersecurity awareness training for all employees

Explanation 280. Correct Answer: C. Enforcing strict access controls based on the principle of least privilege. The principle of least privilege (PoLP) ensures that users are given only the permissions they need to perform their job functions, nothing more. By enforcing strict access controls using this principle, the financial institution can minimize the risk of unauthorized internal users accessing sensitive financial data.

Option A is incorrect. Perimeter firewalls are more focused on preventing external threats and don't specifically address unauthorized internal access.

Option B is incorrect. Implementing 2FA is primarily for authenticating users and doesn't prevent unauthorized internal users from accessing data if they are already authenticated.

Option D is incorrect. While cybersecurity awareness training is crucial, it's not the most effective specific measure to prevent unauthorized internal access to financial data.

Question 281. Alice, a system administrator for a startup, is preparing to deploy a new website for her company. To ensure secure communications between the users and the website, she plans to obtain a digital certificate for the site. Before doing so, which step must Alice first undertake to get a certificate from a Certificate Authority (CA)?

- (A) **Generate a public-private key pair**
- (B) Submit her passport copy to the CA
- (C) Download the latest CA root certificate
- (D) Encrypt the website with symmetric encryption

Explanation 281. Correct Answer: A. Generate a public-private key pair. Before Alice can request a digital certificate from a CA, she must first generate a public-private key pair. Once this is done, she creates a Certificate Signing Request (CSR) containing her public key and some additional information. The CSR is then submitted to the CA for signing.

Option B is incorrect. CAs do not typically require a passport copy for standard SSL/TLS certificates. They might have identity verification processes, but it's usually for extended validation certificates.

Option C is incorrect. While it may be necessary to trust a CA by downloading its root certificate, this is not the step required before requesting a digital certificate.

Option D is incorrect. Symmetric encryption is unrelated to the process of obtaining a digital certificate.

Question 282. TechFin Bank is considering implementing a new software system for their transaction processing. Before rolling it out, the cybersecurity team insists on carrying out a specific type of analysis to understand how this change might affect the organization's security posture. What is the team referring to?

- (A) Risk appetite assessment
- (B) Performance benchmarking
- (C) **Impact analysis**
- (D) Penetration testing

Explanation 282. Correct Answer: C. Impact analysis. An impact analysis assesses the potential consequences of a change within an organization. In the context of TechFin Bank, the cybersecurity team would use this analysis to understand how the new software system might introduce new vulnerabilities, affect existing security measures, or otherwise impact the bank's overall security.

Option A is incorrect. Risk appetite assessment refers to determining the amount and type of risk an organization is willing to accept in pursuit of its objectives. It doesn't focus on the consequences of a specific change.

Option B is incorrect. Performance benchmarking focuses on comparing an organization's performance metrics to industry standards or best practices, not assessing the potential security impact of a change.

Option D is incorrect. While penetration testing is crucial to assess the vulnerabilities in a system, it doesn't provide a

holistic view of the potential impacts a change might have on an organization's security posture.

Question 283. The software development team at ABC Corp. has created a unique application that utilizes innovative algorithms. The company wants to ensure that competitors cannot legally copy or replicate their application's functionality. Which of the following would be the MOST suitable method to protect this intellectual property?

- (A) Copyright the user interface design
- (B) **Apply for a patent for the innovative algorithms**
- (C) Store the application code in an encrypted vault
- (D) Ensure all users sign an acceptable use policy (AUP)

Explanation 283. Correct Answer: B. Apply for a patent for the innovative algorithms. Patents provide legal protection for inventions, allowing the inventor or patent holder the exclusive right to the patented process, design, or invention for a certain period. In this case, patenting the algorithms would prevent competitors from legally replicating the application's unique functionality.

Option A is incorrect. Copyrighting the user interface design would only protect the visual appearance and elements of the application, not its unique functionality or underlying algorithms.

Option C is incorrect. While storing the application code in an encrypted vault protects it from unauthorized access, it does not provide legal protection against replication by competitors if they develop similar functionality independently.

Option D is incorrect. An acceptable use policy (AUP) defines how users are allowed to use the software or system, but it doesn't offer protection against competitors copying the application's unique functionality.

Question 284. SecureBank is in the process of selecting a vendor for their new online transaction system. The bank is keen on ensuring the selected vendor has robust security measures and a track record of maintaining those measures. As part of the vendor selection process, which of the following steps is the most relevant to the bank's concerns?

- (A) Checking the vendor's sales growth over the last five years
- (B) Conducting due diligence regarding the vendor's security practices**
- (C) Comparing the visual appeal of the vendor's user interface to competitors
- (D) Evaluating the vendor's marketing strategies

Explanation 284. Correct Answer: B. Conducting due diligence regarding the vendor's security practices.

Conducting due diligence regarding the vendor's security practices ensures that the bank has a comprehensive understanding of the vendor's security posture and past performance, aligning with the bank's concerns for a robust and secure online transaction system.

Option A is incorrect. While a vendor's sales growth might indicate business success, it does not provide insight into their security measures.

Option C is incorrect. The visual appeal of a user interface does not provide information on the security measures or practices of a vendor.

Option D is incorrect. Evaluating marketing strategies provides no direct insight into the security practices of a vendor.

Question 285. XYZ Corp, a manufacturer of smart home devices, failed to implement standard security practices in their products. A popular tech review site publishes an in-depth review detailing these vulnerabilities. Which of the following outcomes is XYZ Corp MOST likely to face as an immediate result?

- (A) An award for innovation in smart home technologies
- (B) **Reputational damage leading to decreased sales**
- (C) An increased partnership with tech retailers
- (D) A surge in the employee recruitment rate

Explanation 285. Correct Answer: B. Reputational damage leading to decreased sales. Negative reviews, especially those highlighting security vulnerabilities, can lead to a loss of trust among consumers, potentially resulting in decreased sales due to reputational damage.

Option A is incorrect. Receiving an award for innovation is unlikely in the face of publicized security vulnerabilities.

Option C is incorrect. Partnerships with tech retailers might be jeopardized, or at least put on hold, given the negative publicity around the product's security flaws.

Option D is incorrect. A negative review, especially one that underscores security vulnerabilities, is unlikely to boost recruitment. Potential employees may be wary of joining a company with a tarnished reputation.

Question 286. An e-commerce company is experiencing attacks that specifically target the shopping cart feature of its web application. They want to implement a firewall that can understand web application-specific commands and provide protection. Which type of firewall should they consider?

- (A) Layer 4 Firewall
- (B) Layer 2 Firewall
- (C) **Layer 7 Firewall**
- (D) Packet Filtering Firewall

Explanation 286. Correct Answer: C. Layer 7 Firewall.

Layer 7 firewalls, often known as Application Layer firewalls, can understand and filter traffic based on application-specific data, commands, or functions. They operate at the highest layer in the OSI model and can make decisions based on the actual content of the traffic.

Option A is incorrect. Layer 4 firewalls, also known as transport layer firewalls, primarily deal with data based on port numbers and protocol. They wouldn't be as effective in filtering application-specific commands as a Layer 7 firewall.

Option B is incorrect. Layer 2 firewalls operate at the data link layer, primarily dealing with MAC addresses. They aren't equipped to analyze application-specific content.

Option D is incorrect. Packet Filtering Firewalls operate primarily at the network layer, making decisions based on source/destination IP addresses, port numbers, and protocol types, not application-specific content.

Question 287. John, a senior executive at XYZ Corp., gets a call from someone claiming to be from the bank's fraud department. The caller asks John to confirm certain transactions by providing the OTP sent to his registered mobile number. What form of social engineering attack is John likely facing?

- (A) Baiting
- (B) Quizzing
- (C) **Vishing**
- (D) Pharming

Explanation 287. Correct Answer: C. Vishing. Vishing, short for voice phishing, is the act of using the telephone to scam the user into surrendering private information that will be used for identity theft.

Vishing attacks capitalize on trust, using voice calls to manipulate victims into divulging sensitive information. Attackers often pose as legitimate entities or departments, like a bank's fraud department, to make their scam appear genuine.

Option A is incorrect. Baiting involves luring a victim into downloading malicious software under the guise of a free or beneficial download.

Option B is incorrect. Quizzing isn't a recognized type of social engineering attack.

Option D is incorrect. Pharming involves redirecting a website's traffic to a bogus site, often to capture login credentials.

Question 288. DeltaCorp, a retail company, has assessed that a security breach might result in a loss of \$1 million in sales. The company has determined that they can tolerate a loss of up to \$500,000, but anything beyond that would severely impact operations. To cover the potential financial loss beyond their tolerance level, they decide to purchase cybersecurity insurance. Which of the following terms best describes the \$500,000 figure?

- (A) Risk appetite
- (B) **Risk threshold**
- (C) Risk capacity
- (D) Risk assessment

Explanation 288. Correct Answer: B. Risk threshold. The risk threshold is the specific level of risk an organization is willing to accept. In this case, DeltaCorp is willing to accept potential losses up to \$500,000, marking that as their threshold.

Option A is incorrect. Risk appetite is a broader term that reflects the general level of risk an organization is willing to accept in pursuit of its objectives. It's more about strategic intent than specific figures.

Option C is incorrect. Risk capacity refers to the total amount of risk an organization can absorb without significantly impacting its strategic objectives or viability. It's a broader measure than the specific tolerance threshold.

Option D is incorrect. Risk assessment is the process of identifying, analyzing, and evaluating risks. It's not a specific figure or threshold.

Question 289. A financial organization collects and stores personally identifiable information (PII) of its customers. The company operates within jurisdictions that have strict regulations concerning the storage, transmission, and processing of such data. Which of the following strategies would be MOST appropriate for the company to ensure compliance with these regulations?

- (A) Use open source encryption algorithms without validation
- (B) Only store customer data in physical, on-site servers
- (C) **Implement data classification and labeling procedures**
- (D) Limit the number of administrators with access to the data

Explanation 289. Correct Answer: C. Implement data classification and labeling procedures. By implementing data classification and labeling procedures, the organization can clearly identify which data is regulated, ensuring appropriate controls, access rights, and protective measures are in place. This aids in achieving compliance by setting clear guidelines on data handling based on the classification.

Option A is incorrect. While encryption is essential for protecting sensitive data, using open source algorithms without validation might not ensure that the data is protected to the standards required by regulations.

Option B is incorrect. Storing customer data only on physical, on-site servers doesn't necessarily guarantee compliance. Regulations often require specific controls regardless of where the data is stored.

Option D is incorrect. While limiting administrative access can reduce the risk of insider threats, it doesn't directly ensure that the regulated data is handled in compliance with legal requirements.

Question 290. An organization is transitioning its IT infrastructure to be cloud-centric and aims to adopt a zero-trust network approach. They are looking for a solution that integrates cloud security, zero-trust access, and WAN capabilities, ensuring employees have consistent secure access regardless of their location. Which of the following best addresses their needs?

- (A) Remote Desktop Services (RDS)
- (B) **Secure access service edge (SASE)**
- (C) Content Delivery Network (CDN)
- (D) Virtual Local Area Network (VLAN)

Explanation 290. Correct Answer: B. Secure access service edge (SASE). SASE integrates multiple network and security functions traditionally delivered in separate point solutions. This includes capabilities such as Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall-as-a-Service (FWaaS), and Zero Trust Network Access (ZTNA), all delivered from a globally distributed set of cloud-native platforms.

Option A is incorrect. Remote Desktop Services (RDS) enables users to connect to a graphical interface of a remote computer, but it doesn't inherently combine cloud security, zero-trust access, and WAN capabilities like SASE.

Option C is incorrect. A Content Delivery Network (CDN) is designed to deliver web content and web applications to users based on their geographical location. It doesn't provide integrated cloud security and WAN capabilities.

Option D is incorrect. A Virtual Local Area Network (VLAN) segments a physical network into multiple isolated networks. It doesn't offer the combined benefits of cloud security, zero-trust access, and WAN capabilities like SASE.

Question 291. MedTech, a medical device manufacturer, did not adhere to the required standards for device security and patient data protection. Which of the following repercussions might be the MOST critical for MedTech's ongoing operations?

- (A) Increased public relations campaigns
- (B) Short-term stock price fluctuations
- (C) Offering discounts on their devices
- (D) **Loss of license to manufacture and distribute**

Explanation 291. Correct Answer: D. Loss of license to manufacture and distribute. For a medical device manufacturer, maintaining adherence to industry-specific standards is crucial. Non-compliance, especially when it involves patient data protection, can lead to the company losing its license to operate.

Option A is incorrect. While public relations campaigns might be employed to manage reputation, it's not a direct consequence of non-compliance.

Option B is incorrect. Stock price fluctuations could occur due to many factors, but it's not the most critical consequence concerning the company's ability to operate.

Option C is incorrect. Offering discounts might be a strategy to regain customer trust, but it's not a direct result of non-compliance nor is it as critical as the potential loss of a license.

Question 292. A multinational corporation is looking to replace its current firewalls at all its global branches. The IT director wants a solution that can perform stateful inspection of packets, application-level filtering, and integrate threat intelligence feeds for updated threat awareness. Which of the following would be the most suitable solution?

- (A) Stateful Packet Inspection Firewall
- (B) Proxy Server
- (C) Web Application Firewall (WAF)
- (D) **Next-Generation Firewall (NGFW)**

Explanation 292. Correct Answer: D. Next-Generation Firewall (NGFW). Next-Generation Firewalls (NGFWs) are designed to offer traditional firewall capabilities such as stateful inspection but also come with advanced features like application-level filtering and the ability to integrate with threat intelligence feeds. This makes NGFWs suitable for modern, complex environments that demand multi-layered security features.

Option A is incorrect. While a Stateful Packet Inspection Firewall can monitor the state of active connections and analyze the packets, it doesn't offer advanced features like application-level filtering or the integration of threat intelligence feeds that a NGFW does.

Option B is incorrect. A Proxy Server controls and filters requests from clients to servers, typically for web access. It doesn't possess the comprehensive security functionalities of a NGFW.

Option C is incorrect. A Web Application Firewall (WAF) specifically protects web applications from targeted attacks. While valuable, it doesn't offer the breadth of features and integrations that a NGFW does.

Question 293. A security analyst is reviewing a vulnerability report and sees a reference to CVE-2023-12345 with a CVSS score of 9.5. Which of the following conclusions can the analyst draw based on this information?

- (A) **The vulnerability was first identified in the year 2023**
- (B) The vulnerability is of low severity
- (C) The vulnerability affects only software produced in 2023
- (D) CVE-2023-12345 is the software vendor's internal code for the vulnerability

Explanation 293. Correct Answer: A. The vulnerability was first identified in the year 2023. The CVE identifier's format begins with the year the vulnerability was made public, so CVE-2023-12345 indicates a vulnerability identified in 2023.

Option B is incorrect. CVSS scores range from 0 to 10, with higher scores indicating higher severity. A score of 9.5 is considered critical severity, not low.

Option C is incorrect. The year in a CVE identifier refers to when the vulnerability was published, not the year the software was produced.

Option D is incorrect. The CVE system is a standard method for identifying vulnerabilities and doesn't represent a software vendor's internal coding.

Question 294. GlobalTech, a software development company, is entering into a partnership with WebSolutions, a web hosting provider. They aim to create a standard set of terms governing their ongoing business transactions, including payment terms, delivery protocols, and warranties. Which type of agreement is most suitable for establishing these foundational terms for future transactions?

- (A) Memorandum of understanding (MOU)
- (B) Non-disclosure agreement (NDA)
- (C) Licensing agreement
- (D) **Master service agreement (MSA)**

Explanation 294. Correct Answer: D. Master service agreement (MSA). A Master service agreement (MSA) is designed to define a broad framework covering the terms and conditions of business transactions between parties. It sets out general terms so that specific details can be negotiated in subsequent contracts. Given that GlobalTech and WebSolutions

intend to outline foundational terms for their ongoing transactions, an MSA is the most fitting choice.

Option A is incorrect. An MOU establishes mutual intentions but typically doesn't detail specific transaction terms.

Option B is incorrect. An NDA focuses on maintaining confidentiality and doesn't establish transactional terms.

Option C is incorrect. A licensing agreement concerns the rights to use, distribute, or reproduce specific software or intellectual property

Question 295. AlphaTech, a leading IT company, recently identified a critical vulnerability in its primary software product. They have developed a patch to address the vulnerability. Before distributing the patch to its customers, which of the following should AlphaTech ideally perform?

- (A) Deploy the patch on all company systems
- (B) Notify the media about the vulnerability
- (C) **Test the patch in a controlled environment**
- (D) Offer compensation to affected customers

Explanation 295. Correct Answer: C. Test the patch in a controlled environment. Before deploying or distributing a patch, especially for a critical vulnerability, it's essential to test it in a controlled environment. This ensures that the patch doesn't introduce new issues and that it effectively addresses the vulnerability.

Option A is incorrect. Deploying the patch immediately on all company systems without testing it could lead to unforeseen issues or even exacerbate the problem.

Option B is incorrect. Notifying the media about the vulnerability, especially before it's been effectively addressed and without a coordinated disclosure plan, can lead to panic and potential exploitation by malicious actors.

Option D is incorrect. Offering compensation is reactive and doesn't directly address the vulnerability. The primary goal after identifying a vulnerability should be to address and mitigate it.

Question 296. Employees at a renowned software development firm frequently visit an industry-related forum to discuss the latest trends and technologies. Over the past month, several employees reported malware infections shortly after accessing the forum. An investigation suggests the forum was compromised to target the company's developers specifically. Which type of attack most accurately describes this scenario?

- (A) Spear Phishing
- (B) **Watering Hole**
- (C) Drive-by Download
- (D) Whaling

Explanation 296. Correct Answer: B. Watering Hole. The attack focused on a particular site that employees at the targeted organization are known to visit, intending to compromise those specific individuals.

A watering hole attack involves compromising a website or online resource frequented by members of a particular group or organization. Once compromised, attackers can use the site to deploy malware to the targeted individuals.

Option A is incorrect. Spear phishing is a targeted phishing attempt, typically via email, aimed at a specific individual or organization. It does not involve compromising websites that targets frequent.

Option C is incorrect. While a drive-by download might be the method used to deliver malware once the forum was compromised, the overall strategy of targeting a specific site known to be frequented by the victims defines it as a watering hole attack.

Option D is incorrect. Whaling is a type of phishing attack aimed at high-profile targets like CEOs or CFOs. It doesn't involve compromising websites.

Question 297. A cybersecurity firm has been hired by TechGiant Corp. to perform penetration testing on their infrastructure. Before the testing begins, the CEO of TechGiant Corp. wants to ensure that certain critical systems are not targeted, and that the testing will not disrupt their ongoing operations. What should be established to define the scope and boundaries of the test?

- (A) Service-level agreement (SLA)
- (B) Non-disclosure agreement (NDA)
- (C) **Rules of engagement (ROE)**
- (D) Memorandum of understanding (MOU)

Explanation 297. Correct Answer: C. Rules of engagement (ROE). The Rules of Engagement (ROE) document defines the scope, boundaries, methods, and other critical guidelines for a penetration test. It ensures that both the testing team and the organization understand and agree on what can and cannot be done during the testing.

Option A is incorrect. A Service-level agreement (SLA) primarily deals with the levels of service expected, such as uptime, response times, etc. It doesn't define the boundaries of a penetration test.

Option B is incorrect. A Non-disclosure agreement (NDA) is about keeping information confidential and wouldn't define the scope of a penetration test.

Option D is incorrect. A Memorandum of understanding (MOU) is a general agreement between parties, but it doesn't detail the specific scope and rules of a penetration test like the ROE would.

Question 298. During a routine vulnerability assessment, TechInc discovers a weakness in their system that, if exploited, would allow an attacker to modify existing user accounts, including privileges. Which classification best describes this vulnerability?

- (A) **Elevation of privilege vulnerability**
- (B) Disclosure vulnerability
- (C) Replay vulnerability
- (D) Remote code execution vulnerability

Explanation 298. Correct Answer: A. Elevation of privilege vulnerability. Elevation of privilege vulnerabilities allow attackers to increase their privileges within a system, often giving them more access than intended. The scenario describes a situation where user accounts and their privileges can be modified, aligning with this classification.

Option B is incorrect. Disclosure vulnerabilities involve unauthorized access to information but not the modification of user privileges or data.

Option C is incorrect. Replay vulnerabilities occur when attackers capture and later retransmit valid data transmissions to fool a system, which is not described in the given scenario.

Option D is incorrect. Remote code execution vulnerabilities allow attackers to execute arbitrary commands or code on a target system. While these can be severe, the given scenario specifically describes privilege changes, not arbitrary code execution.

Question 299. An e-commerce company is rolling out a new web application to facilitate online payments. The IT department wants to be immediately notified of any application errors or unauthorized modifications to the application's codebase. Which of the following tools should they implement?

- (A) Web Application Firewall (WAF)
- (B) **Application Performance Monitoring (APM)**
- (C) Domain Name System (DNS) monitoring tool
- (D) Network flow analyzer

Explanation 299. Correct Answer: B. Application

Performance Monitoring (APM). APM tools are designed to monitor the performance of applications and can detect application errors, anomalies, and unauthorized code changes, thereby ensuring application stability and security.

Option A is incorrect. While a WAF protects web applications from various cyber threats by filtering and monitoring HTTP traffic, it doesn't typically monitor for application errors or unauthorized code changes.

Option C is incorrect. DNS monitoring tools focus on ensuring the availability and integrity of DNS services and do not monitor application performance or codebase changes.

Option D is incorrect. Network flow analyzers examine data flows on the network but do not specifically monitor application performance or codebase modifications.

Question 300. A security analyst is exploring ways to proactively identify vulnerabilities within the organization's infrastructure. Which of the following provides the BEST method for the analyst to receive real-time threat intelligence from the dark web?

- (A) Utilizing a vulnerability scanner on the organization's internal network
- (B) **Subscribing to a dark web threat intelligence feed**
- (C) Conducting regular penetration tests on external-facing systems
- (D) Reviewing daily reports from the organization's SIEM system

Explanation 300. Correct Answer: B. Subscribing to a dark web threat intelligence feed. Threat intelligence feeds, especially those focusing on the dark web, provide real-time information about emerging threats and vulnerabilities. This proactive approach allows analysts to be aware of potential threats even before they may affect the organization.

Option A is incorrect. While vulnerability scanners are effective at identifying known vulnerabilities within a network, they don't provide real-time threat intelligence from external sources like the dark web.

Option C is incorrect. Penetration tests are indeed useful for identifying vulnerabilities in systems and applications. However, they don't specifically provide threat intelligence from the dark web.

Option D is incorrect. SIEM systems aggregate and analyze log data from various sources to identify and respond to security incidents. While they can alert to current threats within the environment, they don't offer real-time dark web threat intelligence.

EXAM SIMULATOR #4

Questions 301-400

Question 301. A financial institution is implementing a system where customers can verify the integrity of their monthly statements without having access to the original data. Which of the following techniques would be MOST appropriate for this task?

- (A) Encrypting the statements using AES
- (B) Compressing the statements to reduce file size
- (C) Hashing the statements and providing the hash value to the customers
- (D) Tokenizing sensitive data within the statements

Question 302. A company is developing a new video conferencing tool. They want to make sure that all video and audio data transmitted between participants are encrypted and protected from eavesdropping. Which type of encryption should the developers implement to achieve this?

- (A) Endpoint Encryption
- (B) Transport-layer Encryption
- (C) Volume-level Encryption
- (D) Database-level EncryptionAccess Control

Question 303. A global finance firm has recently faced downtime due to unexpected disasters in its main operational region. The firm wishes to have a backup site that would allow

them to continue their operations with minimal downtime and no data loss. Which type of backup site would be the most appropriate for the firm?

- (A) Cold site
- (B) Warm site
- (C) Hot site
- (D) Mobile site

Question 304. During a routine update, a web server application requires a restart. What should the administrator do FIRST to ensure client connections aren't abruptly terminated during the restart?

- (A) Redirect incoming traffic to a backup server
- (B) Increase the server's memory
- (C) Manually terminate all active client sessions
- (D) Check for available patches for the application

Question 305. Kara, a financial analyst, began to notice unusual account activity tied to her credentials. She is sure she hasn't initiated these transactions. Upon further investigation, IT discovered a program on her computer that was recording her keystrokes. What type of malware was found on Kara's computer?

- (A) Ransomware
- (B) Keylogger
- (C) Adware
- (D) Rootkit

Question 306. Your company has recently deployed an update to its CRM application. Post-update, users are experiencing connectivity issues. As a security administrator, which of the

following steps should you take FIRST to address the connectivity problem without causing data loss?

- (A) Restart the application immediately
- (B) Disconnect all users and then restart the application
- (C) Validate the update's integrity and then restart the application
- (D) Reinstall the previous version of the CRM application

Question 307. A software company has developed a new product. They want to release a user manual that details how to use the software, its features, and basic troubleshooting steps. What should be the classification of this user manual?

- (A) Confidential
- (B) Restricted
- (C) Public
- (D) Internal

Question 308. Jake recently ran an old game on his computer that he received from a friend. Shortly after, he discovered that some of his documents were duplicated with slight modifications, and his system's performance was deteriorating. Which kind of malware most likely caused these issues?

- (A) Adware
- (B) Trojan
- (C) Worm
- (D) Virus

Question 309. Caroline, a security analyst, receives an alert that an unfamiliar file has been detected on a mission-critical server. She suspects it might be malware. What is the BEST immediate action Caroline should take regarding this potential threat?

- (A) Delete the file immediately to prevent further damage
- (B) Quarantine the file to prevent it from executing or spreading
- (C) Make a copy of the file for further analysis
- (D) Notify all employees about the suspicious file

Question 310. Alex recently purchased a new laptop. Upon first startup, he noticed multiple pre-installed software applications, most of which he didn't recognize or find necessary. The laptop's performance was slower than expected given its hardware specifications. Which type of software is most likely causing this performance degradation?

- (A) Ransomware
- (B) Bloatware
- (C) Spyware
- (D) Adware

Question 311. Julia, a cybersecurity analyst, notices a recently installed application named "PhotoEditorPro.exe" on a corporate workstation. Upon further inspection, she identifies that this application is silently exfiltrating sensitive company data to an external IP address. Which type of malware is Julia most likely observing?

- (A) Worm
- (B) Ransomware
- (C) Trojan
- (D) Adware

Question 312. Jane, an employee at XYZ Corp, recently noticed that her browser homepage changed unexpectedly, and she's receiving an increasing number of targeted

advertisements. Additionally, there's a new toolbar in her browser that she doesn't remember installing. Based on these symptoms, which type of malware is most likely affecting Jane's computer?

- (A) Ransomware
- (B) Worm
- (C) Spyware
- (D) Botnet

Question 313. A web server hosting the company's e-commerce site is set for an OS upgrade. The upgrade is expected to last 30 minutes. What should be a primary consideration to minimize customer impact due to potential downtime?

- (A) Implementing a load balancer
- (B) Taking a backup of the e-commerce site
- (C) Posting a maintenance notice a week in advance
- (D) Upgrading the server's hardware

Question 314. After a significant cybersecurity incident, ABC Tech revamped its incident response procedures. However, the documentation was not updated to reflect these changes. During a subsequent minor incident, there was confusion regarding the steps to be followed. Which of the following is the MOST direct implication of not updating the incident response documentation?

- (A) The company may have to invest in new cybersecurity tools
- (B) Stakeholders might lose trust in the company's ability to handle incidents
- (C) Incident response might be inconsistent and less effective

(D) ABC Tech may have to hire external consultants for incident response

Question 315. A network administrator has received a new security patch for a mission-critical application. Which of the following is the BEST action to take before applying this patch in the live environment?

- (A)** Apply the patch immediately to ensure system security
- (B)** Notify all users about the upcoming downtime due to the patch
- (C)** Test the patch in a separate testing environment
- (D)** Take a backup of only the mission-critical application

Question 316. During a routine security audit, a company discovered an unauthorized wireless access point using the same SSID as the company's official wireless network. Additionally, this rogue access point was configured without any encryption. What type of wireless attack is this scenario most indicative of?

- (A)** War Driving
- (B)** Wireless Phishing
- (C)** Bluejacking
- (D)** Evil Twin

Question 317. An IT manager is considering solutions to protect data stored on the laptops provided to remote employees. The primary concern is to ensure that the entire content of the laptop's storage drive is unreadable if a laptop is lost or stolen. Which encryption level would best address this concern?

- (A)** File-level Encryption

- (B) Transport-layer Encryption
- (C) Full-disk Encryption
- (D) Database-level Encryption

Question 318. An e-commerce website suddenly experiences a sharp increase in traffic, causing the website to become slow and occasionally inaccessible. The IT team observes that a large number of requests are originating from multiple IP addresses spread across various countries. What type of network attack is the e-commerce website likely experiencing?

- (A) Man-in-the-middle attack
- (B) DNS spoofing
- (C) Distributed denial-of-service (DDoS) attack
- (D) ARP poisoning

Question 319. During a scheduled maintenance window, a security administrator plans to apply a critical update to the company's firewall. Which of the following actions is MOST crucial to ensure minimized downtime during this process?

- (A) Notifying the firewall vendor about the update
- (B) Disabling all firewall rules temporarily
- (C) Creating a rollback plan in case of update failure
- (D) Scheduling the update during peak business hours

Question 320. A global e-commerce website wants to allow its customer service representatives to assist clients with order issues without exposing the full credit card details of the clients. Which method should the IT department employ to achieve this?

- (A) Replace all digits of the credit card number with random characters

- (B) Display only the last four digits of the credit card number while masking the rest
- (C) Encrypt the credit card number with a symmetric key
- (D) Use a hash function to represent the credit card number

Question 321. A security analyst at DataCorp is tasked with preventing unauthorized external applications from connecting to their server. Which approach should the analyst primarily rely on to achieve this?

- (A) Implement an allow list for approved applications
- (B) Monitor server CPU usage
- (C) Regularly patch server software
- (D) Encrypt data at rest on the server

Question 322. Your organization plans to upgrade its database system. To maintain security during this process, which of the following actions should be RESTRICTED until the upgrade is validated?

- (A) Monitoring the database for any anomalies
- (B) Allowing end-users to access the upgraded database
- (C) Making regular backups of the database
- (D) Reviewing the database system logs

Question 323. After a series of system enhancements, a financial organization decided to use a manual method of documenting changes in separate files rather than implementing a version control system. During an audit, the cybersecurity team struggled to determine which version of a critical system file was the most recent and accurate. What is the PRIMARY risk of not implementing version control for such documentation?

- (A) Increased storage requirements for multiple files
- (B) Difficulty in collaborating between team members
- (C) Lack of traceability and difficulty in reverting to a known stable state
- (D) Greater need for training staff on manual documentation

Question 324. Your organization is preparing to upgrade a database server that supports an e-commerce application. A review of the change management documentation has revealed that multiple applications rely on this particular database server for various functionalities. Which of the following steps should be taken FIRST to ensure a smooth upgrade process without disruptions?

- (A) Upgrade the database server immediately to benefit from new features
- (B) Perform a backup of the database server
- (C) Identify and test all applications that have dependencies on the database server
- (D) Inform users about potential downtime during the upgrade

Question 325. A multinational corporation is concerned about the possibility of losing access to encrypted data due to the loss or compromise of private keys. They've approached a third-party organization for a solution. Which of the following is a system that allows the third party to securely hold a copy of the corporation's cryptographic keys to ensure data recoverability?

- (A) Public Key Repository
- (B) Key Generation Center
- (C) Key Escrow
- (D) Key Renewal Service

Question 326. A software developer at XYZ Corp included a piece of code in the company's software that would corrupt the application's databases if his name was ever removed from the list of contributors in the application credits. Months after he left the company, the application databases were corrupted after an update. What type of malware was responsible for this action?

- (A) Trojan
- (B) Spyware
- (C) Adware
- (D) Logic bomb

Question 327. An employee notices a stranger standing unusually close to her with an unfamiliar device while she uses her RFID badge to enter the office building. A few days later, her colleague's badge suddenly stops working, even though it was not reported lost or damaged. What type of attack should the security team suspect?

- (A) Brute force attack on the access control system
- (B) RFID cloning
- (C) Tailgating
- (D) RFID jamming

Question 328. An employee at a large corporation has recently installed an app on his company-issued mobile device from a website instead of the approved app store. The app claimed to help boost productivity, but soon after, sensitive data from the mobile device was found to be transmitted to an unknown server. What mobile vulnerability was exploited?

- (A) Inadequate password policies
- (B) Open Wi-Fi connection

- (C) Mobile device side loading
- (D) Lack of mobile device encryption

Question 329. A user reports that whenever they try to visit their online banking website, they are redirected to a website that looks identical but has a slightly different URL. The fake website asks for additional personal details that the bank never requested before. Which type of DNS attack is the user likely encountering?

- (A) DNS Tunneling
- (B) DNS Fast Flux
- (C) DNS Cache Poisoning
- (D) Domain Hijacking

Question 330. An IT security team received reports that a new, previously unknown vulnerability was being actively exploited in the wild. The software vendor has not yet provided a patch for the vulnerability. What is the most accurate term for this vulnerability?

- (A) Legacy vulnerability
- (B) Zero-day vulnerability
- (C) Patched vulnerability
- (D) Known vulnerability

Question 331. An online payment gateway is evaluating methods to enhance the security of its payment processing system. They want a solution that replaces sensitive cardholder data with a unique identifier that has no intrinsic value by itself. Which method should they implement?

- (A) Hashing the card data
- (B) Encrypting the card data

- (C) Masking the card data
- (D) Tokenizing the card data

Question 332. A multinational corporation communicates sensitive information between its branches using encryption. An internal audit reveals that the encryption algorithms being used are those that were deprecated several years ago. Which of the following cryptographic vulnerabilities is the organization most exposed to?

- (A) Key generation flaw
- (B) Weak algorithms susceptible to attacks
- (C) Inadequate public key infrastructure
- (D) Mismanagement of cryptographic keys

Question 333. During a quarterly review, the IT team at a logistics company decided to change the configuration of their load balancers to better distribute traffic among their servers. After the change, a series of technical issues emerged, affecting customer-facing applications. When troubleshooting the issue, it was discovered that the network diagrams had not been updated to reflect the new changes. What is the MAJOR consequence of not having updated diagrams in such a scenario?

- (A) The servers might need a hardware upgrade
- (B) The company might need to revert to the old load balancer configuration
- (C) It increases the time and complexity of troubleshooting
- (D) Customers might prefer other logistics companies

Question 334. An online banking website employs a system that automatically logs out users after 10 minutes of inactivity to ensure that if a user forgets to log out, no one else can alter

the user's banking details. Which principle of the CIA triad is the banking website MOST directly addressing?

- (A) Confidentiality
- (B) Availability
- (C) Authentication
- (D) Integrity

Question 335. A user, Amy, wants to securely send a confidential document to her colleague, Bob. Amy decides to encrypt the document to ensure its confidentiality. Which of the following should Amy use to encrypt the document, ensuring only Bob can decrypt it?

- (A) Amy's private key
- (B) Amy's public key
- (C) Bob's private key
- (D) Bob's public key

Question 336. A tech startup is developing a mobile application that offers exclusive content only to users within a specific country due to licensing agreements. Which method should the startup use to ensure that only users within that country can access the content?

- (A) Integrate a time-based one-time password (TOTP) system
- (B) Use geolocation-based access controls
- (C) Enable biometric authentication
- (D) Implement IP whitelisting

Question 337. An organization's IT department noticed a rapid increase in network traffic over the past 24 hours. Simultaneously, many employees reported that their systems

have been slow and that they received a file named “updatePatch.exe” from coworkers via email, even though the coworkers did not intentionally send any files. What type of malware is most likely responsible for this behavior?

- (A) Trojan
- (B) Ransomware
- (C) Adware
- (D) Worm

Question 338. A software development company maintains a shared code repository. The company wants to ensure that only developers can make changes to the code, but testers should be able to view the code without modifying it. Which approach should be implemented?

- (A) Assign all employees read-only permissions
- (B) Provide testers with administrative rights
- (C) Implement role-based access controls (RBAC)
- (D) Use data encryption on the repository

Question 339. An organization recently deployed a cloud-based database to support its new application. A few weeks later, unauthorized access to the database was detected. An investigation revealed that the database was accessible without a password. Which of the following misconfigurations is primarily responsible for the security breach?

- (A) Default configurations left unchanged
- (B) Insufficient network segmentation
- (C) Encryption not enabled at rest
- (D) Lack of intrusion detection system

Question 340. During a routine security review, a security analyst discovers multiple failed login attempts to a secure server room's electronic access control system, all within a short time span. The access logs show a sequential pattern of access codes being tried. What type of physical attack is likely being attempted?

- (A) Tailgating
- (B) Phishing
- (C) Brute force
- (D) Social engineering

Question 341. A multinational e-commerce company is expanding its infrastructure to handle increasing traffic. The primary goal is to distribute the incoming web traffic across multiple servers to ensure that no single server is overwhelmed. Which method should the company use?

- (A) Deploy a web application firewall
- (B) Implement server clustering
- (C) Use hardware-based firewalls
- (D) Set up a load balancer

Question 342. Alice needs to provide proof of the authenticity of a digital document she's sending to Bob. Which of the following cryptographic elements should Alice use to accomplish this task and ensure Bob knows the document came from her?

- (A) Encrypt the document with Bob's private key
- (B) Encrypt the document with her public key
- (C) Sign the document with her private key
- (D) Sign the document with Bob's public key

Question 343. Sarah, a cybersecurity analyst, receives a report that a company laptop was stolen from an employee's car. The laptop contained sensitive financial data. Sarah checked the company's security configurations and found that the laptop was equipped with full-disk encryption. How does this impact the potential data breach situation?

- (A) The data remains easily accessible, as only the boot sector was encrypted
- (B) The data is protected, as the entire hard drive's contents are encrypted
- (C) The data is partially encrypted, with only the user directories protected
- (D) The data is vulnerable since full-disk encryption only applies when the laptop is connected to the company network

Question 344. A large news website was rendered unavailable during a major news event. Network logs show an overwhelming amount of traffic from IoT devices. Which type of DDoS attack leveraged IoT devices is this indicative of?

- (A) Reflected Attack
- (B) Botnet Attack
- (C) Amplification Attack
- (D) Teardrop Attack

Question 345. A security administrator needs to apply a configuration change to a critical service, requiring a service restart. Before initiating the restart, which of the following steps is MOST important to ensure continuous service availability?

- (A) Implement automatic service restart on failure
- (B) Announce the restart to all company employees

- (C) Schedule the restart during off-peak hours
- (D) Take a backup of the current service configuration

Question 346. The finance department at a large firm still relies on a legacy application for their quarterly reporting. This application is known to have some security flaws, but due to its critical nature, it cannot be easily replaced. How can the firm BEST mitigate the risks associated with this application?

- (A) Train the finance team about the latest cybersecurity threats
- (B) Run the legacy application on the latest hardware to improve performance
- (C) Place the legacy application behind a web application firewall (WAF)
- (D) Frequently change the passwords of users who have access to the application

Question 347. A company is preparing to roll out a new infrastructure deployment for its internal network. They have a server that will store both highly confidential customer information and non-sensitive marketing material. The IT department wants to ensure that only the confidential data is encrypted, while the marketing data remains easily accessible. Which level of encryption would be most suitable for this scenario?

- (A) File-level Encryption
- (B) Full-disk Encryption
- (C) Partition Encryption
- (D) Transport-layer Encryption

Question 348. An organization's security team discovered that an attacker had gained unauthorized access to a server. Upon investigating, they found a software tool that allowed the attacker to mask processes, files, and system data, effectively remaining hidden while maintaining privileged access. What type of malware was implanted by the attacker?

- (A) Trojan
- (B) Worm
- (C) Logic Bomb
- (D) Rootkit

Question 349. As part of an initial penetration testing phase, Jackson is using tools that directly probe and interact with the target system's network to discover open ports, services, and other potential access points. While this approach is more direct and could be detected by the target's security systems, it provides detailed and actionable insights. Which type of reconnaissance is Jackson performing?

- (A) Threat analysis
- (B) Passive reconnaissance
- (C) Active reconnaissance
- (D) Social engineering

Question 350. HealthCareNow, a large hospital chain, wants to ensure its newly implemented electronic health record (EHR) system adheres to national standards. Which type of audit would be most appropriate to confirm that HealthCareNow is in compliance with national regulations regarding patient data?

- (A) Self-assessment using internal standards
- (B) Third-party risk assessment

- (C) External regulatory audit
- (D) Informal peer review

Question 351. A healthcare provider stores vast amounts of patient data on its servers. While they have strong perimeter defenses, they want an additional layer of security to ensure patient data remains confidential even in the event of unauthorized access. Which of the following would be the MOST effective solution for this requirement?

- (A) Use hash algorithms on all patient data
- (B) Implement data deduplication techniques
- (C) Encrypt the stored patient data
- (D) Use a web application firewall (WAF)

Question 352. John, a citizen of a country that strictly follows the General Data Protection Regulation (GDPR), used a global online shopping platform for a year. He decided to stop using the platform and requested the deletion of all his personal data. What is the online platform's primary obligation concerning John's request under the "Right to be Forgotten" principle?

- (A) Retain the data but ensure that John's data is never used for marketing purposes
- (B) Delete all personal data about John unless there's a legal reason to keep it
- (C) Anonymize John's data and notify him of the completion
- (D) Move John's data to a secure, encrypted server where it won't be accessed

Question 353. TechFirm, a leading technology conglomerate, recently conducted a security exercise. The goal was for the

internal security team to defend against a series of simulated attacks from an external red team. While the red team launched attacks, the internal team's objective was to detect, respond, and mitigate those threats. What type of penetration testing is TechFirm employing for its internal security team?

- (A) Offensive penetration testing
- (B) Passive penetration testing
- (C) Defensive penetration testing
- (D) Black box testing

Question 354. During a security assessment of an application, Ryan found that he was able to input larger-than-expected data into a field. Upon doing so, he noticed the application became unresponsive and eventually crashed. What type of vulnerability might Ryan have uncovered?

- (A) Input Validation Error
- (B) Cross-Site Scripting (XSS)
- (C) Buffer Overflow
- (D) Insecure Direct Object Reference (IDOR)

Question 355. A financial institution wants to ensure that if a cyber attacker gains unauthorized access to one section of their network, the attacker cannot easily move laterally to more sensitive parts of the network. Which method can help achieve this objective?

- (A) Deploying a honeypot in every segment
- (B) Implementing network segmentation
- (C) Applying encryption on all data traffic
- (D) Enabling two-factor authentication for all users

Question 356. Emily, an executive assistant, receives a phone call from an individual claiming to be a new employee in the IT department. The caller says they're conducting a routine check and needs Emily to confirm her username and password for system verification. How should Emily respond?

- (A) Politely decline and report the call to the IT department
- (B) Provide the caller with the username but not the password
- (C) Ask the caller to email the request, so there's a written record
- (D) Hang up without saying anything

Question 357. SafeNet, a financial institution, decided to undertake a comprehensive security assessment. They brought together their internal security team and an external group of ethical hackers. Their objective was for these teams to collaboratively assess vulnerabilities, perform real-time attack simulations, and evaluate defense mechanisms. What form of penetration testing is SafeNet utilizing?

- (A) Black box testing
- (B) Integrated penetration testing
- (C) Defensive penetration testing
- (D) Red team assessment

Question 358. A company's proprietary algorithm is being targeted by competitors aiming to replicate its functionality. To safeguard its intellectual property without changing the algorithm's behavior, the company wants a method that disguises the original code structure. What should they implement?

- (A) Data masking on the algorithm's output

- (B) Obfuscation on the algorithm's code
- (C) Encryption of the algorithm's storage location
- (D) Implementing a hashing mechanism within the algorithm

Question 359. AlphaTech, a leading tech manufacturer, is considering a penetration test to identify vulnerabilities in their new product's firmware. They provide the testers with firmware source code, architecture diagrams, and other internal details to ensure a thorough evaluation. What kind of penetration test is AlphaTech commissioning?

- (A) Zero-knowledge testing
- (B) Open box testing
- (C) Opaque testing
- (D) Blind testing

Question 360. Lisa, a cybersecurity analyst, is setting up a centralized system to correlate logs from multiple sources, detect malicious activities in real-time, and produce comprehensive security reports. Which tool should Lisa consider for this purpose?

- (A) Network Intrusion Detection System (NIDS)
- (B) Web Application Firewall (WAF)
- (C) Vulnerability Scanner
- (D) Security Information and Event Management (SIEM)

Question 361. WebMasters LLC, a popular web hosting company, wants to ensure the robust security of their hosted websites. They initiate a security challenge, inviting ethical hackers worldwide to find vulnerabilities without giving any details about their servers, databases, or applications. Which

penetration testing method is WebMasters LLC utilizing?

- (A) External testing
- (B) Grey box testing
- (C) Active testing
- (D) Black box testing

Question 362. After an annual review, BestTech Co. realized that their IT team was unfamiliar with the protocols to follow during a data breach. To ensure the team understands the steps and decision points without launching a live drill, what should the company implement?

- (A) Upgrade their firewall systems
- (B) Engage in a tabletop exercise
- (C) Conduct a red team exercise
- (D) Implement multi-factor authentication for all users

Question 363. A medium-sized organization recently had a third-party auditor review their information security controls. After the review, the auditor provided a formal statement that verified the effectiveness of the controls in place. What is this formal statement referred to as?

- (A) Certification
- (B) Accreditation
- (C) Attestation
- (D) Assurance

Question 364. In preparation for an upcoming audit, AlphaTech Corporation hires a team to evaluate their security measures. The team is spotted attempting to bypass security barriers, unlock doors without keys, and trying to access restricted floors by pretending to be maintenance staff. What type of testing is

AlphaTech Corporation undergoing?

- (A) Network vulnerability scanning
- (B) Physical penetration testing
- (C) OS fingerprinting
- (D) Source code review

Question 365.. WebSoft Inc., a leading software company, recently launched a new web application. Before making it live, they engaged a security firm to challenge the application, find vulnerabilities, and exploit them as real hackers would. This aggressive testing is done to ensure maximum security. What kind of penetration testing is WebSoft Inc. opting for?

- (A) White box testing
- (B) Defensive penetration testing
- (C) Offensive penetration testing
- (D) Gray box testing

Question 366. After a series of high-profile data breaches in the industry, OnlineRetail Corp., an e-commerce platform, wishes to undergo an external review to validate the security of its operations and provide a comprehensive report to its shareholders. Which type of assessment will provide a detailed and formalized examination of their security posture?

- (A) External examination of IT controls and operations
- (B) Internal review of security protocols
- (C) External regulatory audit on financial statements
- (D) Informal feedback from industry peers

Question 367. XYZ Ltd. wants to evaluate if their current security measures are consistent with industry-specific regulations they are required to follow. The evaluation should

be done by their own IT department before inviting external auditors. Which approach should XYZ Ltd. adopt?

- (A) Third-party vulnerability scanning
- (B) Internal compliance assessment
- (C) External attestation
- (D) Vendor risk assessment

Question 368. SafeNet Banking Corporation is keen on gaining a competitive edge in the market by demonstrating its commitment to cybersecurity. They want an official attestation that their cybersecurity measures are robust and compliant with industry standards. What should SafeNet opt for to obtain this attestation?

- (A) Feedback from customers on the bank's app security
- (B) Internal IT team's report on cybersecurity practices
- (C) External independent third-party audit
- (D) Informal evaluation by a cybersecurity consultancy

Question 369. The company's security administrator observes that there are multiple unauthorized access attempts originating from IP addresses in a specific range. The administrator wants to prevent these IP addresses from accessing the corporate network temporarily. Which of the following firewall configurations would BEST address this requirement?

- (A) Configure an implicit deny rule for the specific IP range
- (B) Set up a honeypot for the specific IP range
- (C) Allow the IP range but set a bandwidth limit
- (D) Add the IP range to a whitelist

Question 370. Lisa, a security administrator, is using a popular benchmark to ensure the web servers in her organization are

configured securely. She wants to make sure that unnecessary services are disabled, and appropriate permissions are set.

Which of the following organizations is MOST likely the source of the benchmark she is using?

- (A) PCI DSS
- (B) OWASP
- (C) CIS
- (D) GDPR

Question 371. ZenTech, a multinational corporation, recently adopted a multi-cloud strategy, deploying workloads across multiple cloud service providers. What is a primary security benefit of this approach?

- (A) Centralized management of all cloud resources
- (B) Automatic encryption of data in transit between clouds
- (C) Mitigation against a single point of failure
- (D) Reduction in the cost of cloud storage solutions

Question 372. A company wants to host a public-facing website but ensure that even if the website gets compromised, attackers cannot gain access to sensitive internal data. Which of the following is the BEST configuration to achieve this?

- (A) Place the web server on the internal network and strictly monitor the traffic
- (B) Place the web server in the DMZ with a firewall in front of it and another firewall between the DMZ and the internal network
- (C) Directly connect the web server to the internet without a firewall and move sensitive data off the server
- (D) Place the web server in the DMZ and connect it directly to the internal network without a firewall

Question 373. TechFirm Inc. collects personal data from its users and decides on the purposes and means of processing this data. They also outsource data storage to CloudData, a third-party company. In the context of data privacy regulations, how would TechFirm and CloudData be classified respectively?

- (A) TechFirm: Processor; CloudData: Controller
- (B) TechFirm: Controller; CloudData: Processor
- (C) Both TechFirm and CloudData: Processors
- (D) Both TechFirm and CloudData: Controllers

Question 374. The IT department of Globex Corp is concerned about the increasing number of malicious websites being accessed from company laptops while employees are working remotely. They want to ensure that the web filter policies set in the corporate network are enforced even when devices are offsite. What would be the BEST solution to address this concern?

- (A) Implement a cloud-based web filtering solution
- (B) Use a VPN to force all remote traffic through the corporate network
- (C) Deploy an agent-based web filter on all company laptops
- (D) Periodically send reminders to employees about acceptable web usage

Question 375. SoftTech Solutions is a software development company that has decided to conduct a penetration test on their new web application. The testers are provided with user credentials, network topology diagrams, and some proprietary software code snippets. Which type of penetration testing is SoftTech Solutions employing?

- (A) Black box testing
- (B) Double-blind testing
- (C) Known environment testing
- (D) Zero-knowledge testing

Question 376. DeltaTech, a financial institution, operates its primary site on a UNIX-based platform. For disaster recovery purposes, they are considering setting up a backup site on a different platform. Which of the following is NOT a primary benefit of introducing platform diversity in this case?

- (A) It reduces the organization's learning curve by using familiar technologies
- (B) It provides resilience against attacks targeting UNIX-based systems
- (C) It ensures that platform-specific outages don't affect both primary and backup sites
- (D) It diversifies the attack surface, reducing the impact of specific platform vulnerabilities

Question 377. After a recent security incident, Sarah, a network security analyst, wants to analyze the flow data of network traffic to identify patterns and potential threats. She wants to collect metadata about IP traffic flow and gather details like IP addresses, ports, and protocols used. Which tool should Sarah employ to obtain this information?

- (A) Intrusion Detection System (IDS)
- (B) Syslog server
- (C) NetFlow collector
- (D) Simple Network Management Protocol (SNMP) traps

Question 378. A large financial institution recently experienced a security breach where an attacker was able to bypass its intrusion detection system (IDS). Upon investigation, the security team found out that the attacker utilized a zero-day exploit. In the aftermath, what should the institution do to enhance the capability of its IDS?

- (A) Switch from a signature-based IDS to a behavior-based IDS
- (B) Disable the IDS and rely solely on firewall rules
- (C) Update the IDS with the latest threat intelligence feeds and signatures
- (D) Reduce the frequency of IDS signature updates

Question 379. After a major power outage, TechWave Corp. wants to ensure their primary data center's operations can be swiftly and seamlessly shifted to another facility. The company wants this process to be automated and immediate to prevent any service interruption. What type of test should TechWave Corp. conduct to validate this functionality?

- (A) Conduct a vulnerability assessment on both data centers
- (B) Execute a failover test
- (C) Engage in a tabletop exercise
- (D) Perform a routine backup test

Question 380. Sarah, a security administrator, is implementing a monitoring solution for her organization's server infrastructure. She wants a solution that does not require any additional software to be installed on the servers themselves. Which type of monitoring approach should Sarah choose?

- (A) Agent-based monitoring
- (B) Intrusion Detection System (IDS)

- (C) Agentless monitoring
- (D) Network-based Application Performance Monitoring (APM)

Question 381. Alice, a cybersecurity analyst, is tasked with identifying potential weaknesses in a newly deployed web application's infrastructure before it goes live. She wants a tool that can proactively discover and report on system vulnerabilities, missing patches, and misconfigurations. Which of the following should Alice utilize for this purpose?

- (A) Intrusion Detection System (IDS)
- (B) Network sniffer
- (C) Vulnerability scanner
- (D) Security Information and Event Management (SIEM) system

Question 382. After conducting a business impact analysis, a local library determined that they could afford several days of downtime without a significant impact on their operations. They want a disaster recovery solution that offers a balance between cost and recovery capabilities. Which site consideration is the most suitable for the library's needs?

- (A) Mobile site with a full set of IT equipment
- (B) Hot site with daily data replication
- (C) Cold site
- (D) Warm site with weekly backups

Question 383. After a recent security incident in the organization, the IT team noticed that several legitimate activities were being flagged by the intrusion detection system, resulting in a high number of false positives. What is the MOST

appropriate action to improve the system's accuracy and reduce unnecessary alerts?

- (A) Disable the intrusion detection system for a week to observe regular network traffic patterns
- (B) Set up a stricter firewall rule to block all external traffic
- (C) Implement alert tuning to refine the system's detection criteria
- (D) Encourage employees to reduce their internet usage

Question 384. Amy, a network administrator, is researching tools to assist with automating the evaluation of her organization's systems against a specific security baseline. She comes across SCAP and wants to implement it. Which of the following BEST describes the primary function of the Security Content Automation Protocol (SCAP)?

- (A) To facilitate the real-time transfer of threat intelligence feeds
- (B) To provide an interface for user authentication against Active Directory
- (C) To allow for automated vulnerability management and policy compliance evaluation
- (D) To offer encrypted communication channels for remote system management

Question 385. A financial institution wants to ensure that any unauthorized access to customer data triggers an immediate alert to the security team. Which of the following approaches would be the MOST effective in achieving this requirement?

- (A) Configure alerts for any modification to database records
- (B) Set up alerts for successful logins during off-business

hours

- (C) Establish alerting thresholds based on anomalous user behavior
- (D) Send daily reports of all access attempts to the security team for review

Question 386. After the recent cyber-attack on Acme Corp, the IT security team decided to enhance their proactive defense mechanism. They want to start with identifying unpatched and vulnerable systems on their network. Which of the following scanning activities would BEST assist them in this endeavor?

- (A) Conducting a passive scan during business hours
- (B) Implementing a full open port scan on all systems
- (C) Running a credentialed vulnerability scan on their network
- (D) Scanning the external perimeter for domain name resolutions

Question 387. A healthcare provider wants to evaluate the security of their patient portal. They inform the penetration testers about the technologies used, such as the programming languages and databases. However, specifics about the security measures in place, including intrusion detection systems, are kept secret. What kind of penetration test are they aiming for?

- (A) White box testing
- (B) External testing
- (C) Grey box testing
- (D) Active testing

Question 388. Sarah, a sales manager at TechWorld Inc., receives an email from her bank urging her to update her

account details due to a recent security breach. The email provides a link to a website that looks almost identical to her bank's official site. However, she notices a slight misspelling in the URL. What should Sarah do next?

- (A) Forward the email to her colleagues as a warning
- (B) Click the link and update her details as the bank's site is probably just undergoing updates
- (C) Delete the email without taking any action
- (D) Report the email to her company's IT department and avoid clicking any links

Question 389. Paul, a network administrator, has configured various networking devices in his organization to send alerts in the event of specific failures. After a switch experienced a power supply failure, Paul received an immediate notification. Which of the following did Paul most likely utilize to receive this notification?

- (A) Syslog server
- (B) Simple Network Management Protocol (SNMP) traps
- (C) Packet sniffer
- (D) Firewall logs

Question 390. Samantha, a security analyst, has been tasked with creating a monthly report for senior management detailing the security posture of the company. Which of the following is the MOST important element to include to ensure the report effectively communicates the company's current security status?

- (A) Detailed technical logs of all security incidents
- (B) Graphical representation of incidents by category
- (C) A complete list of all users and their access levels
- (D) Copies of recent phishing emails for demonstration

Question 391. A software developer in a company notices that a legitimate software tool they use is repeatedly flagged and quarantined by the company's security solution. Which of the following is the BEST action the cybersecurity team can take to address this without compromising security?

- (A) Turn off the antivirus solution
- (B) Whitelist the software tool in the antivirus settings
- (C) Decrease the security level of the antivirus
- (D) Install a different antivirus solution

Question 392. Lucy, the IT security manager of a financial company, receives an automated alert that an employee attempted to email a document containing social security numbers to an external email address. Which of the following tools most likely generated this alert?

- (A) Network Intrusion Detection System (NIDS)
- (B) Data Loss Prevention (DLP) solution
- (C) Vulnerability Scanner
- (D) Packet Analyzer

Question 393. A healthcare organization with patients worldwide is planning to set up a backup site for its medical data repository. They have been advised to consider geographic dispersion as part of their disaster recovery plan. Which of the following reasons is the LEAST valid for geographic dispersion in this scenario?

- (A) Mitigate risks of regional natural disasters
- (B) Offer redundancy in case of local power outages
- (C) Benefit from varying peak load times in different regions
- (D) Ensure faster access speeds for global patients

Question 394. TechCo, a medium-sized enterprise, is planning to implement a solution to monitor, control, and restrict web access for its employees to improve productivity and enhance security. They also want to cache frequently accessed web content to reduce bandwidth consumption. Which solution would BEST fit TechCo's requirements?

- (A) Deploy a decentralized proxy on each departmental network
- (B) Set up a DNS-based filtering service
- (C) Use a centralized proxy with caching capabilities
- (D) Recommend browser extensions for web filtering to all employees

Question 395. A software development company has just expanded its team and wants to ensure that in the event of a disaster, they can resume operations within a day. However, they have a limited budget for disaster recovery. Which of the following disaster recovery site types would be the most suitable for the company's needs?

- (A) Hot site with hourly data replication
- (B) Cold site with monthly data backups
- (C) Warm site with daily backups
- (D) Offsite tape backups

Question 396. A company has recently noticed an increased number of employees accessing social media sites during work hours, leading to decreased productivity. To counter this, the security administrator decides to limit access to these websites during peak working hours. Which firewall rule modification should the administrator make?

- (A) Implement an Intrusion Prevention System (IPS) rule to

block social media content

- (B) Change the firewall rule to deny access to known social media IP addresses between 9 AM and 5 PM
- (C) Use the firewall's URL filtering capability to blacklist social media URLs
- (D) Increase the firewall's bandwidth to accommodate the excess traffic

Question 397. As part of the annual security training, the IT department of XYZ Corp decides to launch a simulated phishing campaign. The aim is to assess employees' ability to identify and report phishing emails. Which of the following would be the MOST effective first step in ensuring the success of this campaign?

- (A) Informing all employees about the campaign a week prior
- (B) Creating a realistic phishing email that closely resembles common threats
- (C) Offering rewards to employees who click on the simulated phishing links
- (D) Reviewing the results of the previous year's campaign

Question 398. An organization is planning to deploy a new web application that will be accessible from both the internal network and the internet. The application will communicate exclusively over HTTPS. The security administrator is asked to configure the firewall to allow the necessary traffic. Which of the following should the administrator configure?

- (A) Allow port 21 and block all others
- (B) Allow port 443 and block all others

- (C) Allow port 80 and block all others
- (D) Allow port 23 and block all others

Question 399. The IT department of XYZ Corp is keen on preventing users from changing specific system settings, such as altering the firewall configurations. The majority of their infrastructure is based on Windows operating systems. Which of the following would be the most effective way to achieve this?

- (A) Use SELinux to enforce strict access controls
- (B) Utilize Group Policy to set and enforce policies related to system settings
- (C) Deploy a third-party software solution to lock system settings
- (D) Implement a user training program to guide users on system settings best practices

Question 400. During a routine check, an IT technician notices several files on a company server have been renamed with a “.locked” extension and there’s a new file named “README_TO_RECOVER_FILES.txt” present in the root directory. Based on these indicators, which type of malicious activity is most likely in progress?

- (A) Worm propagation
- (B) Trojan horse execution
- (C) Ransomware attack
- (D) Logic bomb activation

Answers 301-400

Question 301. A financial institution is implementing a system where customers can verify the integrity of their monthly statements without having access to the original data. Which of the following techniques would be MOST appropriate for this task?

- (A) Encrypting the statements using AES
- (B) Compressing the statements to reduce file size
- (C) **Hashing the statements and providing the hash value to the customers**
- (D) Tokenizing sensitive data within the statements

Explanation 301. Correct Answer: C. Hashing the statements and providing the hash value to the customers.

Hashing can be used to ensure data integrity. Customers can hash the statement they receive and compare it with the provided hash value to verify that the data hasn't been altered.

Option A is incorrect. While AES is a strong encryption method, encrypting the statements won't allow customers to verify the integrity of their statements. It ensures confidentiality more than integrity.

Option B is incorrect. Compressing the statements merely reduces the file size for ease of storage or transmission; it doesn't help in verifying data integrity.

Question 302. A company is developing a new video conferencing tool. They want to make sure that all video and audio data transmitted between participants are encrypted and protected from eavesdropping. Which type of encryption should the developers implement to achieve this?

- (A) Endpoint Encryption
- (B) **Transport-layer Encryption**
- (C) Volume-level Encryption
- (D) Database-level EncryptionAccess Control

Explanation 302. Correct Answer: B. Transport-layer Encryption. Transport-layer Encryption is tailored for securing data while it's in transit. By implementing this encryption, the company ensures that all video and audio data during the video conference are confidential, maintaining the privacy of the participants.

Option A is incorrect. Endpoint Encryption is designed for data on specific devices like laptops or mobile phones, not for data being transmitted over networks.

Option C is incorrect. Volume-level Encryption pertains to encrypting specific logical drives or volumes, not data in transit.

Option D is incorrect. Database-level Encryption secures data within a database and is not specific to data transmission over networks.

Question 303. A global finance firm has recently faced downtime due to unexpected disasters in its main operational region. The firm wishes to have a backup site that would allow them to continue their operations with minimal downtime and no data loss. Which type of backup site would be the most appropriate for the firm?

- (A) Cold site
- (B) Warm site

- (C) **Hot site**
- (D) Mobile site

Explanation 303. Correct Answer: C. Hot site. A hot site is a fully operational offsite data center configured and ready to continue operations immediately after a disaster. It has all the necessary equipment and up-to-date data backups, making it ideal for scenarios where minimal downtime and no data loss are essential.

Option A is incorrect. A cold site is a backup facility with space and infrastructure but without updated equipment or data. It requires time to set up and is not suitable for immediate recovery.

Option B is incorrect. A warm site is a middle ground between a cold and hot site. It has some equipment and backups but will require more time to get fully operational compared to a hot site.

Option D is incorrect. A mobile site is usually a portable setup, often on a truck, that can be deployed to various locations. It might not be equipped for large-scale operations like a global finance firm would require.

Question 304. During a routine update, a web server application requires a restart. What should the administrator do FIRST to ensure client connections aren't abruptly terminated during the restart?

- (A) **Redirect incoming traffic to a backup server**
- (B) Increase the server's memory

- (C) Manually terminate all active client sessions
- (D) Check for available patches for the application

Explanation 304. Correct Answer: A. Redirect incoming traffic to a backup server. Redirecting incoming traffic ensures that clients are not abruptly disconnected and instead can continue their activities on a backup server while the primary server undergoes a restart.

Option B is incorrect. Increasing server memory might improve performance but doesn't address the immediate issue of the service restart.

Option C is incorrect. Manually terminating client sessions would cause abrupt disconnections, which is what the administrator is trying to avoid.

Option D is incorrect. While checking for patches is important, it doesn't address the issue of ensuring client connections aren't terminated during a service restart.

Question 305. Kara, a financial analyst, began to notice unusual account activity tied to her credentials. She is sure she hasn't initiated these transactions. Upon further investigation, IT discovered a program on her computer that was recording her keystrokes. What type of malware was found on Kara's computer?

- (A) Ransomware
- (B) **Keylogger**
- (C) Adware
- (D) Rootkit

Explanation 305. Correct Answer: B. Keylogger. A keylogger is a type of malicious software designed to capture and record the keystrokes of a user without their knowledge, often leading to unauthorized access to sensitive information such as usernames, passwords, and other confidential details.

Option A is incorrect. Ransomware is malware that encrypts a user's data and demands payment for its decryption. It doesn't record keystrokes.

Option C is incorrect. Adware delivers unwanted ads to the user. It doesn't record keystrokes.

Option D is incorrect. A rootkit provides stealthy access to a computer, allowing an attacker to maintain privileged access without detection. It doesn't specifically record keystrokes.

Question 306. Your company has recently deployed an update to its CRM application. Post-update, users are experiencing connectivity issues. As a security administrator, which of the following steps should you take FIRST to address the connectivity problem without causing data loss?

- (A) Restart the application immediately
- (B) Disconnect all users and then restart the application
- (C) **Validate the update's integrity and then restart the application**
- (D) Reinstall the previous version of the CRM application

Explanation 306. Correct Answer: C. Validate the update's integrity and then restart the application. Before making any changes, it's essential to ensure the update's integrity. This

means confirming that the update was correctly applied and that there were no issues during its installation. Once the update's integrity is confirmed, a restart can help apply any changes that may not have taken effect immediately.

Option A is incorrect. Restarting the application immediately without validation might cause further complications if the update was not correctly applied.

Option B is incorrect. While disconnecting users might be necessary at some point, doing so without validating the update's integrity can result in further disruptions.

Option D is incorrect. Reinstalling the previous version is a drastic step and might not be necessary if the update's integrity can be validated and issues resolved with a restart.

Question 307. A software company has developed a new product. They want to release a user manual that details how to use the software, its features, and basic troubleshooting steps. What should be the classification of this user manual?

- (A) Confidential
- (B) Restricted
- (C) **Public**
- (D) Internal

Explanation 307. Correct Answer: C. Public. A user manual is intended for all users of the software and should be easily accessible. It doesn't contain sensitive or proprietary information about the software's underlying code or algorithms. Hence, it should be classified as "Public."

Option A is incorrect. “Confidential” classification is too restrictive for a document meant to be distributed with every software copy and to guide users.

Option B is incorrect. “Restricted” would limit the distribution of the manual unnecessarily, making it harder for users to access the information they need.

Option D is incorrect. “Internal” classification would suggest the manual is only for internal company use, whereas it’s intended for all users of the software.

Question 308. Jake recently ran an old game on his computer that he received from a friend. Shortly after, he discovered that some of his documents were duplicated with slight modifications, and his system’s performance was deteriorating. Which kind of malware most likely caused these issues?

- (A) Adware
- (B) Trojan
- (C) Worm
- (D) **Virus**

Explanation 308. Correct Answer: D. Virus. Viruses are malicious programs that attach to clean files and can replicate, leading to multiple instances of themselves. They can modify or corrupt these files and can degrade system performance as they propagate.

Option A is incorrect. Adware primarily focuses on delivering unwanted advertisements to the user. While it can be annoying, it doesn’t typically duplicate or modify documents.

Option B is incorrect. Trojans are malicious software that disguises themselves as legitimate programs. While they can perform a variety of malicious actions, they don't self-replicate or modify files in the manner described.

Option C is incorrect. Worms are self-replicating malware that spread across networks. While they can cause performance issues, they don't typically attach to files and modify them as viruses do.

Question 309. Caroline, a security analyst, receives an alert that an unfamiliar file has been detected on a mission-critical server. She suspects it might be malware. What is the BEST immediate action Caroline should take regarding this potential threat?

- (A) Delete the file immediately to prevent further damage
- (B) **Quarantine the file to prevent it from executing or spreading**
- (C) Make a copy of the file for further analysis
- (D) Notify all employees about the suspicious file

Explanation 309. Correct Answer: B. Quarantine the file to prevent it from executing or spreading. Quarantining suspicious files isolates them, preventing potential execution or spread while allowing further investigation without immediate deletion.

Option A is incorrect. While deleting the file seems proactive, it removes the chance for further analysis and can affect forensic investigations.

Option C is incorrect. Making a copy is important for analysis, but the immediate priority should be to prevent potential execution or spread of the suspicious file. Quarantine first, then analyze.

Option D is incorrect. Notifying all employees about a specific suspicious file may cause panic or confusion. It's more appropriate to manage the incident first and then communicate relevant information in a structured manner.

Question 310. Alex recently purchased a new laptop. Upon first startup, he noticed multiple pre-installed software applications, most of which he didn't recognize or find necessary. The laptop's performance was slower than expected given its hardware specifications. Which type of software is most likely causing this performance degradation?

- (A) Ransomware
- (B) **Bloatware**
- (C) Spyware
- (D) Adware

Explanation 310. Correct Answer: B. Bloatware. Bloatware refers to unnecessary software applications that come pre-installed on new computers. These applications often consume system resources, leading to reduced performance. Manufacturers sometimes pre-install these applications for promotional purposes or due to partnerships with software providers.

Option A is incorrect. Ransomware encrypts a user's files and demands payment for their decryption. It doesn't come pre-installed on new computers.

Option C is incorrect. Spyware covertly collects information from a system without the user's knowledge. It doesn't typically come pre-installed on new devices as bloatware does.

Option D is incorrect. Adware automatically displays or downloads advertising material on a computer. While it might be annoying, it's not typically pre-installed software that comes with new computers aimed at degrading performance.

Question 311. Julia, a cybersecurity analyst, notices a recently installed application named "PhotoEditorPro.exe" on a corporate workstation. Upon further inspection, she identifies that this application is silently exfiltrating sensitive company data to an external IP address. Which type of malware is Julia most likely observing?

- (A) Worm
- (B) Ransomware
- (C) Trojan
- (D) Adware

Explanation 311. Correct Answer: C. Trojan. A Trojan is a type of malware that disguises itself as a legitimate software or application. Unlike viruses, Trojans don't replicate themselves, but they can be just as destructive if not more so. In this case, the "PhotoEditorPro.exe" appears to be a legitimate photo editing application but is actually being used to transmit sensitive data to an external source.

Option A is incorrect. Worms are malware programs that replicate themselves to spread to other devices. They don't typically disguise themselves as legitimate applications.

Option B is incorrect. Ransomware encrypts the victim's data and demands a ransom to decrypt it. It doesn't disguise itself as legitimate software.

Option D is incorrect. Adware is software that displays unwanted advertisements. It doesn't typically exfiltrate data or disguise itself as legitimate software.

Question 312. Jane, an employee at XYZ Corp, recently noticed that her browser homepage changed unexpectedly, and she's receiving an increasing number of targeted advertisements. Additionally, there's a new toolbar in her browser that she doesn't remember installing. Based on these symptoms, which type of malware is most likely affecting Jane's computer?

- (A) Ransomware
- (B) Worm
- (C) **Spyware**
- (D) Botnet

Explanation 312. Correct Answer: C. Spyware. Spyware is a type of malware that covertly collects information from a user's system. Changes to browser settings, such as a new homepage or a new toolbar, combined with targeted advertisements, are common indicators that spyware might be present on a system.

Option A is incorrect. Ransomware is malware that encrypts a user's files and demands payment for their release. The described symptoms do not align with ransomware behavior.

Option B is incorrect. Worms are a type of malware that self-replicate and spread across networks. They typically don't modify browser settings or show targeted advertisements.

Option D is incorrect. A botnet involves a collection of internet-connected devices, which may have been infected with malware, being used to perform coordinated tasks. It doesn't directly result in the browser-based symptoms described.

Question 313. A web server hosting the company's e-commerce site is set for an OS upgrade. The upgrade is expected to last 30 minutes. What should be a primary consideration to minimize customer impact due to potential downtime?

- (A) **Implementing a load balancer**
- (B) Taking a backup of the e-commerce site
- (C) Posting a maintenance notice a week in advance
- (D) Upgrading the server's hardware

Explanation 313. Correct Answer: A. Implementing a load balancer. A load balancer can redirect traffic to other servers while one is undergoing maintenance, ensuring that customers can still access the e-commerce site and minimizing the impact of downtime. Load balancers distribute incoming traffic across multiple servers, allowing one server to be taken offline without affecting the availability of the service.

Option B is incorrect. While backups are crucial for disaster recovery, they don't minimize immediate downtime during upgrades.

Option C is incorrect. While informing customers is a good practice, it doesn't prevent downtime. Some customers may still try to access the site during maintenance.

Option D is incorrect. Upgrading the server's hardware might improve performance but doesn't directly minimize the downtime caused by an OS upgrade.

Question 314. After a significant cybersecurity incident, ABC Tech revamped its incident response procedures. However, the documentation was not updated to reflect these changes. During a subsequent minor incident, there was confusion regarding the steps to be followed. Which of the following is the MOST direct implication of not updating the incident response documentation?

- (A) The company may have to invest in new cybersecurity tools
- (B) Stakeholders might lose trust in the company's ability to handle incidents
- (C) **Incident response might be inconsistent and less effective**
- (D) ABC Tech may have to hire external consultants for incident response

Explanation 314. Correct Answer: C. Incident response might be inconsistent and less effective. Without up-to-date documentation reflecting the most recent incident response

procedures, there's a risk that the response will be inconsistent, leading to inefficiencies and potential oversights.

Option A is incorrect. While new tools might be beneficial, the direct concern with outdated documentation is the effectiveness of the response.

Option B is incorrect. While stakeholder trust is important, the immediate implication of outdated documentation is the quality of the incident response.

Option D is incorrect. Hiring external consultants might be an option, but the direct consequence of outdated documentation is the potential ineffectiveness of the internal response process.

Question 315. A network administrator has received a new security patch for a mission-critical application. Which of the following is the BEST action to take before applying this patch in the live environment?

- (A) Apply the patch immediately to ensure system security
- (B) Notify all users about the upcoming downtime due to the patch
- (C) **Test the patch in a separate testing environment**
- (D) Take a backup of only the mission-critical application

Explanation 315. Correct Answer: C. Test the patch in a separate testing environment. Testing any changes, including patches, in a separate environment before deploying them to production is essential to ensure there are no unintended technical implications. This is a key aspect of change

management processes and helps prevent system outages or vulnerabilities from being introduced.

Option A is incorrect. While applying patches is crucial for maintaining security, doing so immediately without proper testing can lead to unforeseen technical problems.

Option B is incorrect. Notifying users is important, but it's premature to notify them without first testing the patch.

Option D is incorrect. Taking a backup is a good practice, but it is not a substitute for testing the patch first.

Question 316. During a routine security audit, a company discovered an unauthorized wireless access point using the same SSID as the company's official wireless network. Additionally, this rogue access point was configured without any encryption. What type of wireless attack is this scenario most indicative of?

- (A) War Driving
- (B) Wireless Phishing
- (C) Bluejacking
- (D) **Evil Twin**

Explanation 316. Correct Answer: D. Evil Twin. An "Evil Twin" attack involves setting up a rogue wireless access point that mimics a legitimate access point. By doing so, an attacker can intercept, monitor, and manipulate the traffic of users who mistakenly connect to the rogue access point.

Option A is incorrect. War Driving involves driving around areas to discover wireless networks and possibly exploit them. It doesn't necessarily involve creating rogue access points.

Option B is incorrect. Wireless Phishing is not a standard term in wireless network security. Phishing generally involves tricking users into revealing sensitive information through deceptive websites or emails.

Option C is incorrect. Bluejacking involves sending unsolicited messages to Bluetooth-enabled devices. It's not related to wireless networks (Wi-Fi).

Question 317. An IT manager is considering solutions to protect data stored on the laptops provided to remote employees. The primary concern is to ensure that the entire content of the laptop's storage drive is unreadable if a laptop is lost or stolen. Which encryption level would best address this concern?

- (A) File-level Encryption
- (B) Transport-layer Encryption
- (C) **Full-disk Encryption**
- (D) Database-level Encryption

Explanation 317. Correct Answer: C. Full-disk Encryption.

Full-disk Encryption (FDE) encrypts the entire storage drive, making all data on the drive unreadable without the correct decryption key or credentials. This is especially useful for portable devices like laptops, which are more vulnerable to physical theft.

Option A is incorrect. File-level Encryption encrypts individual files rather than the entire disk, so some data or system files might remain unencrypted.

Option B is incorrect. Transport-layer Encryption protects data in transit, not data at rest on storage drives.

Option D is incorrect. Database-level Encryption encrypts data within a database and does not apply to other files or data outside of that database.

Question 318. An e-commerce website suddenly experiences a sharp increase in traffic, causing the website to become slow and occasionally inaccessible. The IT team observes that a large number of requests are originating from multiple IP addresses spread across various countries. What type of network attack is the e-commerce website likely experiencing?

- (A) Man-in-the-middle attack
- (B) DNS spoofing
- (C) **Distributed denial-of-service (DDoS) attack**
- (D) ARP poisoning

Explanation 318. Correct Answer: C. Distributed denial-of-service (DDoS) attack. In a DDoS attack, the attacker uses multiple systems, often compromised ones from different locations, to flood a target system with requests, making the target slow or inaccessible.

Option A is incorrect. A man-in-the-middle attack involves an attacker secretly intercepting and possibly altering the

communication between two parties. It doesn't lead to website inaccessibility due to high traffic.

Option B is incorrect. DNS spoofing is when an attacker introduces corrupt DNS cache information to redirect traffic to a different IP address, usually under the attacker's control. It doesn't cause increased traffic from various countries.

Option D is incorrect. ARP poisoning is a technique by which an attacker sends fake ARP messages onto a local area network. This is usually used to link an attacker's MAC address with the IP address of another host, causing any traffic meant for that IP address to be sent to the attacker instead.

Question 319. During a scheduled maintenance window, a security administrator plans to apply a critical update to the company's firewall. Which of the following actions is MOST crucial to ensure minimized downtime during this process?

- (A) Notifying the firewall vendor about the update
- (B) Disabling all firewall rules temporarily
- (C) **Creating a rollback plan in case of update failure**
- (D) Scheduling the update during peak business hours

Explanation 319. Correct Answer: C. Creating a rollback plan in case of update failure. In change management processes, having a rollback plan ensures that if there are issues with the applied update, the system can be reverted to its previous state, thereby minimizing downtime.

Option A is incorrect. While it might be useful to notify the firewall vendor, it is not the most crucial step to minimize downtime.

Option B is incorrect. Disabling all firewall rules can introduce significant security risks and might not be related directly to the downtime.

Option D is incorrect. Scheduling updates during peak business hours could result in maximum disruption and downtime.

Question 320. A global e-commerce website wants to allow its customer service representatives to assist clients with order issues without exposing the full credit card details of the clients. Which method should the IT department employ to achieve this?

- (A) Replace all digits of the credit card number with random characters
- (B) **Display only the last four digits of the credit card number while masking the rest**
- (C) Encrypt the credit card number with a symmetric key
- (D) Use a hash function to represent the credit card number

Explanation 320. Correct Answer: B. Display only the last four digits of the credit card number while masking the rest.

Displaying only the last four digits and masking the rest ensures that customer service representatives have enough information to assist customers without being exposed to the entire credit card number.

Option A is incorrect. Replacing all digits with random characters would render the information useless for customer service representatives as they would not have any reference point.

Option C is incorrect. Encrypting the card number can protect the data, but the customer service representatives would need a way to decrypt it to access even partial information, defeating the purpose of not exposing them to the full details.

Option D is incorrect. Hashing the number would not allow any portion of the original data, like the last four digits, to be viewed, making it ineffective for this use case.

Question 321. A security analyst at DataCorp is tasked with preventing unauthorized external applications from connecting to their server. Which approach should the analyst primarily rely on to achieve this?

- (A) **Implement an allow list for approved applications**
- (B) Monitor server CPU usage
- (C) Regularly patch server software
- (D) Encrypt data at rest on the server

Explanation 321. Correct Answer: A. Implement an allow list for approved applications. By implementing an allow list, the analyst can specify which applications are authorized to connect to the server. Any application not on the list will be prevented from establishing a connection, effectively stopping unauthorized external applications.

Option B is incorrect. While monitoring server CPU usage can provide insights into the server's performance and potential anomalies, it doesn't prevent unauthorized applications from connecting.

Option C is incorrect. Regularly patching server software is a best practice for security to fix known vulnerabilities. However, patching doesn't directly prevent specific external applications from connecting.

Option D is incorrect. Encrypting data at rest helps protect stored data from unauthorized access but does not regulate which applications can connect to the server.

Question 322. Your organization plans to upgrade its database system. To maintain security during this process, which of the following actions should be RESTRICTED until the upgrade is validated?

- (A) Monitoring the database for any anomalies
- (B) **Allowing end-users to access the upgraded database**
- (C) Making regular backups of the database
- (D) Reviewing the database system logs

Explanation 322. Correct Answer: B. Allowing end-users to access the upgraded database. Until the upgraded system is validated and any potential issues are addressed, end-user access should be restricted. This ensures that any vulnerabilities or problems introduced by the upgrade don't compromise data or allow unauthorized activities.

Option A is incorrect. Monitoring the database is crucial to identify any potential security issues and should not be restricted.

Option C is incorrect. Regular backups should continue, as they are part of a comprehensive disaster recovery and data protection strategy.

Option D is incorrect. Reviewing logs is essential to monitor the system's health and security; hence, it should not be restricted.

Question 323. After a series of system enhancements, a financial organization decided to use a manual method of documenting changes in separate files rather than implementing a version control system. During an audit, the cybersecurity team struggled to determine which version of a critical system file was the most recent and accurate. What is the PRIMARY risk of not implementing version control for such documentation?

- (A) Increased storage requirements for multiple files
- (B) Difficulty in collaborating between team members
- (C) **Lack of traceability and difficulty in reverting to a known stable state**
- (D) Greater need for training staff on manual documentation

Explanation 323. Correct Answer: C. Lack of traceability and difficulty in reverting to a known stable state. Version control provides a clear history of changes, ensuring easy reversion to a known stable state, and identifying the latest version of a document or system file. In the absence of version

control, identifying the most recent and accurate version can be challenging.

Option A is incorrect. While storage might be a concern, the primary risk is the inability to trace changes and revert to a stable state.

Option B is incorrect. Collaboration might be hindered, but the direct risk is associated with traceability and stability.

Option D is incorrect. Training staff is always essential, but the immediate concern is the ability to trace and manage changes.

Question 324. Your organization is preparing to upgrade a database server that supports an e-commerce application. A review of the change management documentation has revealed that multiple applications rely on this particular database server for various functionalities. Which of the following steps should be taken FIRST to ensure a smooth upgrade process without disruptions?

- (A) Upgrade the database server immediately to benefit from new features
- (B) Perform a backup of the database server
- (C) **Identify and test all applications that have dependencies on the database server**
- (D) Inform users about potential downtime during the upgrade

Explanation 324. Correct Answer: C. Identify and test all applications that have dependencies on the database server.

Before making changes, especially to systems with multiple dependencies, it's crucial to understand the full scope of potential impacts. By identifying and testing all dependent applications, you ensure that the upgrade won't inadvertently disrupt other services or functionalities.

Option A is incorrect. Upgrading immediately without considering dependencies can lead to unforeseen disruptions and complications.

Option B is incorrect. While backing up the server is a good practice, understanding dependencies should come first to plan the upgrade effectively.

Option D is incorrect. Informing users is essential, but understanding the upgrade's potential impact should come first to provide accurate information.

Question 325. A multinational corporation is concerned about the possibility of losing access to encrypted data due to the loss or compromise of private keys. They've approached a third-party organization for a solution. Which of the following is a system that allows the third party to securely hold a copy of the corporation's cryptographic keys to ensure data recoverability?

- (A) Public Key Repository
- (B) Key Generation Center
- (C) **Key Escrow**
- (D) Key Renewal Service

Explanation 325. Correct Answer: C. Key Escrow. Key escrow is a system in which cryptographic keys are securely

stored with a third party, so they can be retrieved in cases where the original keys are lost or compromised. This ensures data recoverability while maintaining security.

Option A is incorrect. A Public Key Repository is where public keys are stored for retrieval, not for backup or recovery purposes.

Option B is incorrect. Key Generation Center is responsible for creating cryptographic keys, not storing them for recovery purposes.

Option D is incorrect. Key Renewal Service deals with replacing and updating cryptographic keys as they expire or need refreshing, not storing them for recovery.

Question 326. A software developer at XYZ Corp included a piece of code in the company's software that would corrupt the application's databases if his name was ever removed from the list of contributors in the application credits. Months after he left the company, the application databases were corrupted after an update. What type of malware was responsible for this action?

- (A) Trojan
- (B) Spyware
- (C) Adware
- (D) **Logic bomb**

Explanation 326. Correct Answer: D. Logic bomb. A logic bomb is a type of malware that is triggered by a specific event

or condition. In this case, the software developer's name being removed from the contributors triggered the malicious code.

Option A is incorrect. A Trojan disguises itself as legitimate software but performs malicious activities once installed. The scenario does not describe behavior characteristic of a Trojan.

Option B is incorrect. Spyware is designed to collect and send information, typically without the user's knowledge. It does not corrupt databases based on specific triggers.

Option C is incorrect. Adware delivers unwanted advertisements to the user. It does not take malicious actions based on specific events.

Question 327. An employee notices a stranger standing unusually close to her with an unfamiliar device while she uses her RFID badge to enter the office building. A few days later, her colleague's badge suddenly stops working, even though it was not reported lost or damaged. What type of attack should the security team suspect?

- (A) Brute force attack on the access control system
- (B) **RFID cloning**
- (C) Tailgating
- (D) RFID jamming

Explanation 327. Correct Answer: B. RFID cloning. RFID cloning involves making an unauthorized copy of an RFID badge or tag by capturing its signal. The stranger standing unusually close with a device might have been capturing the RFID signal to clone it.

Option A is incorrect. While a brute force attack on an access control system involves trying multiple combinations to gain access, the scenario does not describe multiple access attempts or any involvement with the system itself.

Option C is incorrect. Tailgating involves following an authorized individual into a secure area without the proper credentials. The scenario describes a potential RFID capture, not someone following another person.

Option D is incorrect. RFID jamming would involve interfering with the RFID signal to prevent it from working, not copying the RFID details for unauthorized use.

Question 328. An employee at a large corporation has recently installed an app on his company-issued mobile device from a website instead of the approved app store. The app claimed to help boost productivity, but soon after, sensitive data from the mobile device was found to be transmitted to an unknown server. What mobile vulnerability was exploited?

- (A) Inadequate password policies
- (B) Open Wi-Fi connection
- (C) **Mobile device side loading**
- (D) Lack of mobile device encryption

Explanation 328. Correct Answer: C. Mobile device side loading. Side loading refers to the practice of installing apps on a mobile device from sources other than the approved app store. This can expose the device to apps that have not been vetted for security, leading to potential data compromise, as described in the scenario.

Option A is incorrect. While inadequate password policies can expose a device to unauthorized access, the scenario specifically mentions an app installed from an unapproved source, which points to side loading.

Option B is incorrect. An open Wi-Fi connection can expose mobile devices to threats, but the main issue described in the scenario revolves around the installation of an app from an unapproved source.

Option D is incorrect. While mobile device encryption is essential to protect data, the issue in the scenario is related to side loading, not the encryption status of the device.

Question 329. A user reports that whenever they try to visit their online banking website, they are redirected to a website that looks identical but has a slightly different URL. The fake website asks for additional personal details that the bank never requested before. Which type of DNS attack is the user likely encountering?

- (A) DNS Tunneling
- (B) DNS Fast Flux
- (C) **DNS Cache Poisoning**
- (D) Domain Hijacking

Explanation 329. Correct Answer: C. DNS Cache Poisoning. DNS Cache Poisoning, also known as DNS spoofing, involves corrupting the DNS cache data in DNS resolvers to redirect users to malicious websites instead of the actual intended websites.

Option A is incorrect. DNS Tunneling is a technique where non-DNS traffic is encapsulated in DNS protocols. It's a way to bypass network security but doesn't usually lead to the described redirection scenario.

Option B is incorrect. DNS Fast Flux involves rapidly changing the IP address associated with a domain name to hide the malicious server behind it. It is used to prevent the malicious domain from being taken down but doesn't cause redirection to a similar-looking site.

Option D is incorrect. Domain Hijacking involves an attacker taking control of a domain by altering its registration data without the owner's permission. While this could lead to a similar outcome, the scenario describes a situation where only certain users are redirected, not all visitors to the domain.

Question 330. An IT security team received reports that a new, previously unknown vulnerability was being actively exploited in the wild. The software vendor has not yet provided a patch for the vulnerability. What is the most accurate term for this vulnerability?

- (A) Legacy vulnerability
- (B) **Zero-day vulnerability**
- (C) Patched vulnerability
- (D) Known vulnerability

Explanation 330. Correct Answer: B. Zero-day vulnerability. A zero-day vulnerability refers to a flaw in software, hardware, or firmware that is unknown to the vendor. This type of vulnerability is a risk because there is no fix or

patch for it at the time of discovery, and it may already be actively exploited by malicious actors.

Option A is incorrect. A legacy vulnerability typically refers to a vulnerability in older software or systems that might not be supported anymore, not necessarily an unknown and unpatched flaw.

Option C is incorrect. A patched vulnerability implies that there's already a fix available for the flaw. In the scenario provided, no patch has been released yet.

Option D is incorrect. While the vulnerability may become known to some entities, such as the security team in this scenario, it remains unknown to the software vendor. Thus, “known vulnerability” is not the most accurate descriptor in this context.

Question 331. An online payment gateway is evaluating methods to enhance the security of its payment processing system. They want a solution that replaces sensitive cardholder data with a unique identifier that has no intrinsic value by itself. Which method should they implement?

- (A) Hashing the card data
- (B) Encrypting the card data
- (C) Masking the card data
- (D) **Tokenizing the card data**

Explanation 331. Correct Answer: D. Tokenizing the card data. Tokenization involves replacing sensitive data with a non-

sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value.

Option A is incorrect. Hashing would produce a fixed-size string, which cannot be reversed to its original value, but it doesn't create a "token" that can be swapped back for the original data.

Option B is incorrect. Encryption translates data into another form, or code, so that only people with access to a secret key or password can read it. It does not replace the data with a unique identifier with no intrinsic value.

Option C is incorrect. Masking involves hiding parts of data, such as showing only the last four digits of a credit card number. It doesn't replace the data with a unique identifier.

Question 332. A multinational corporation communicates sensitive information between its branches using encryption. An internal audit reveals that the encryption algorithms being used are those that were deprecated several years ago. Which of the following cryptographic vulnerabilities is the organization most exposed to?

- (A) Key generation flaw
- (B) **Weak algorithms susceptible to attacks**
- (C) Inadequate public key infrastructure
- (D) Mismanagement of cryptographic keys

Explanation 332. Correct Answer: B. Weak algorithms susceptible to attacks. When an organization is found to be using deprecated or older encryption algorithms, it means they

are relying on cryptographic methods that might have known vulnerabilities or could be easier to break due to advancements in computing and cryptanalysis. Over time, certain algorithms are found to have weaknesses and are replaced with more robust ones.

Option A is incorrect. The scenario does not specify issues with key generation but rather focuses on the use of outdated encryption algorithms.

Option C is incorrect. There's no information in the scenario suggesting problems with the organization's public key infrastructure.

Option D is incorrect. While key management is crucial, the primary issue presented in the scenario revolves around the usage of weak or outdated algorithms.

Question 333. During a quarterly review, the IT team at a logistics company decided to change the configuration of their load balancers to better distribute traffic among their servers. After the change, a series of technical issues emerged, affecting customer-facing applications. When troubleshooting the issue, it was discovered that the network diagrams had not been updated to reflect the new changes. What is the MAJOR consequence of not having updated diagrams in such a scenario?

- (A) The servers might need a hardware upgrade
- (B) The company might need to revert to the old load balancer configuration
- (C) **It increases the time and complexity of**

troubleshooting

(D) Customers might prefer other logistics companies

Explanation 333. Correct Answer: C. It increases the time and complexity of troubleshooting. Accurate and up-to-date documentation, including network diagrams, is crucial for effective troubleshooting. Without it, IT teams can spend unnecessary time trying to understand the current state of the system, delaying the resolution of the issue.

Option A is incorrect. While server upgrades might be necessary in some cases, it's not a direct consequence of outdated diagrams.

Option B is incorrect. Reverting to an old configuration might be a potential solution, but the primary issue is the increased troubleshooting complexity due to outdated documentation.

Option D is incorrect. While the potential loss of customers can be an indirect consequence of prolonged technical issues, the immediate concern of outdated diagrams is the impact on troubleshooting.

Question 334. An online banking website employs a system that automatically logs out users after 10 minutes of inactivity to ensure that if a user forgets to log out, no one else can alter the user's banking details. Which principle of the CIA triad is the banking website MOST directly addressing?

(A) Confidentiality

(B) Availability

- (C) Authentication
- (D) Integrity

Explanation 334. Correct Answer: D. Integrity. The integrity pillar of the CIA triad ensures the accuracy and reliability of data. By logging out users after a period of inactivity, the banking website aims to prevent unauthorized modifications (potentially by someone else who might gain access to the unattended session) to the user's banking details, thereby maintaining the integrity of the data.

Option A is incorrect. While logging out users does have a confidentiality aspect, the primary aim in this scenario is to prevent unauthorized changes rather than unauthorized viewing.

Option B is incorrect. Availability ensures that data and systems are accessible to authorized users when they need it. This scenario doesn't discuss providing or restricting access based on system uptime or accessibility.

Option C is incorrect. Authentication ensures that users are who they claim to be. While the scenario does touch on security measures, the primary concern here is preventing unauthorized changes to data, which aligns with integrity, not authentication.

Question 335. A user, Amy, wants to securely send a confidential document to her colleague, Bob. Amy decides to encrypt the document to ensure its confidentiality. Which of the following should Amy use to encrypt the document, ensuring only Bob can decrypt it?

- (A) Amy's private key

- (B) Amy's public key
- (C) Bob's private key
- (D) **Bob's public key**

Explanation 335. Correct Answer: D. Bob's public key. In asymmetric encryption, if a message is encrypted with an individual's public key, only the corresponding private key can decrypt it. Therefore, to ensure Bob is the only person who can decrypt the document, Amy should encrypt it using Bob's public key.

Option A is incorrect. Encrypting with Amy's private key would allow anyone with Amy's public key to decrypt it, and it would also serve as a digital signature rather than ensuring confidentiality.

Option B is incorrect. Using Amy's public key would not make sense because then only Amy's private key could decrypt it.

Option C is incorrect. The private key should never be shared or used for encryption. Its main use is for decryption and signing.

Question 336. A tech startup is developing a mobile application that offers exclusive content only to users within a specific country due to licensing agreements. Which method should the startup use to ensure that only users within that country can access the content?

- (A) Integrate a time-based one-time password (TOTP) system

- (B) Use geolocation-based access controls
- (C) Enable biometric authentication
- (D) Implement IP whitelisting

Explanation 336. Correct Answer: B. Use geolocation-based access controls. Geolocation-based access controls can identify a user's geographic location and allow or deny access based on predefined geographic boundaries, making it the most suitable solution for the startup's requirement.

Option A is incorrect. TOTP systems provide a second factor of authentication based on time, not geographic location.

Option C is incorrect. Biometric authentication verifies the identity of a user based on physical or behavioral characteristics but does not restrict access based on geography.

Option D is incorrect. IP whitelisting allows access only to specific IP addresses. While it can offer a level of geographic restriction, it's not as precise as geolocation-based controls and may inadvertently block or allow users.

Question 337. An organization's IT department noticed a rapid increase in network traffic over the past 24 hours.

Simultaneously, many employees reported that their systems have been slow and that they received a file named "updatePatch.exe" from coworkers via email, even though the coworkers did not intentionally send any files. What type of malware is most likely responsible for this behavior?

- (A) Trojan
- (B) Ransomware

- (C) Adware
- (D) **Worm**

Explanation 337. Correct Answer: D. Worm. Worms are a type of malware that self-replicates and spreads to other devices. The rapid increase in network traffic and the distribution of a file to various users without the sender's knowledge is characteristic of worm behavior. They can consume bandwidth and system resources, causing systems to slow down.

Option A is incorrect. A Trojan disguises itself as legitimate software but does not replicate itself or send itself via email like worms do.

Option B is incorrect. Ransomware encrypts files on a victim's computer and demands a ransom for the decryption key. It doesn't self-replicate and spread like a worm.

Option C is incorrect. Adware primarily serves unwanted ads to users and doesn't replicate itself to spread to other systems.

Question 338. A software development company maintains a shared code repository. The company wants to ensure that only developers can make changes to the code, but testers should be able to view the code without modifying it. Which approach should be implemented?

- (A) Assign all employees read-only permissions
- (B) Provide testers with administrative rights
- (C) **Implement role-based access controls (RBAC)**
- (D) Use data encryption on the repository

Explanation 338. Correct Answer: C. Implement role-based access controls (RBAC). RBAC assigns permissions based on roles within an organization. Developers can be given a role that allows them to modify code, while testers are given a role that only allows them to read the code.

Option A is incorrect. Assigning read-only permissions to all employees will prevent developers from making necessary changes to the code.

Option B is incorrect. Providing testers with administrative rights would give them more access than necessary, potentially allowing them to modify the code.

Option D is incorrect. While data encryption ensures the confidentiality of the data, it does not address the need for specific permission levels for different user roles.

Question 339. An organization recently deployed a cloud-based database to support its new application. A few weeks later, unauthorized access to the database was detected. An investigation revealed that the database was accessible without a password. Which of the following misconfigurations is primarily responsible for the security breach?

- (A) **Default configurations left unchanged**
- (B) Insufficient network segmentation
- (C) Encryption not enabled at rest
- (D) Lack of intrusion detection system

Explanation 339. Correct Answer: A. Default configurations left unchanged. The scenario describes a situation where a

cloud-based database was accessible without a password. This is a common oversight when default configurations, which may have no password or a widely known default password, are left unchanged upon deployment.

Option B is incorrect. While network segmentation is crucial for security, the primary issue in this scenario is the database's lack of password protection, not its network placement.

Option C is incorrect. Though encryption at rest is a best practice for data protection, the immediate issue here is unauthorized access due to a lack of password, not data exposure from the database's stored data.

Option D is incorrect. An intrusion detection system (IDS) might have detected the unauthorized access sooner, but the core vulnerability was the unchanged default configurations.

Question 340. During a routine security review, a security analyst discovers multiple failed login attempts to a secure server room's electronic access control system, all within a short time span. The access logs show a sequential pattern of access codes being tried. What type of physical attack is likely being attempted?

- (A) Tailgating
- (B) Phishing
- (C) **Brute force**
- (D) Social engineering

Explanation 340. Correct Answer: C. Brute force. A brute force attack involves trying every possible combination in an

attempt to find the correct one. The sequential pattern of access codes being tried in the logs suggests that the attacker is systematically going through all potential combinations.

Option A is incorrect. Tailgating involves an attacker following an authorized person into a secure area without the proper credentials. It doesn't involve multiple electronic access code attempts.

Option B is incorrect. Phishing is a type of social engineering attack that typically involves tricking someone into divulging their credentials or other sensitive information. It doesn't involve direct physical access attempts.

Option D is incorrect. While social engineering does involve manipulating individuals to gain unauthorized access, it is not specific to a brute force attack on an electronic system.

Question 341. A multinational e-commerce company is expanding its infrastructure to handle increasing traffic. The primary goal is to distribute the incoming web traffic across multiple servers to ensure that no single server is overwhelmed. Which method should the company use?

- (A) Deploy a web application firewall
- (B) Implement server clustering
- (C) Use hardware-based firewalls
- (D) **Set up a load balancer**

Explanation 341. Correct Answer: D. Set up a load balancer. Load balancers distribute incoming traffic across multiple

servers to ensure that no single server is overwhelmed, which enhances the availability and fault tolerance of applications.

Option A is incorrect. While a web application firewall can protect against web-based threats, it doesn't distribute incoming traffic across servers.

Option B is incorrect. Server clustering primarily focuses on providing redundancy and failover capabilities rather than distributing incoming traffic.

Option C is incorrect. Hardware-based firewalls are primarily used to filter traffic and protect networks from external threats, not to distribute incoming web traffic.

Question 342. Alice needs to provide proof of the authenticity of a digital document she's sending to Bob. Which of the following cryptographic elements should Alice use to accomplish this task and ensure Bob knows the document came from her?

- (A) Encrypt the document with Bob's private key
- (B) Encrypt the document with her public key
- (C) **Sign the document with her private key**
- (D) Sign the document with Bob's public key

Explanation 342. Correct Answer: C. Sign the document with her private key. To prove authenticity, a digital signature is created using the sender's private key. When Bob receives the document, he can verify the signature using Alice's public key. This proves that the document was signed by Alice and has not been tampered with during transit.

Option A is incorrect. Bob's private key is known only to Bob and should never be used by anyone else, including for encryption.

Option B is incorrect. Encrypting with Alice's public key doesn't prove authenticity. It would also mean only Alice's private key could decrypt it, which isn't the intent.

Option D is incorrect. One does not sign documents with the recipient's public key. Signatures are created using the sender's private key.

Question 343. Sarah, a cybersecurity analyst, receives a report that a company laptop was stolen from an employee's car. The laptop contained sensitive financial data. Sarah checked the company's security configurations and found that the laptop was equipped with full-disk encryption. How does this impact the potential data breach situation?

- (A) The data remains easily accessible, as only the boot sector was encrypted
- (B) The data is protected, as the entire hard drive's contents are encrypted**
- (C) The data is partially encrypted, with only the user directories protected
- (D) The data is vulnerable since full-disk encryption only applies when the laptop is connected to the company network

Explanation 343. Correct Answer: B. The data is protected, as the entire hard drive's contents are encrypted. Full-disk Encryption (FDE) encrypts the entirety of a hard drive, ensuring that all its contents, including system and user files, are

unreadable without the appropriate decryption key or credentials. As such, even if the laptop is stolen, the data remains secured unless the attacker has the decryption key.

Option A is incorrect. Full-disk Encryption does not encrypt only the boot sector; it encrypts the entire disk.

Option C is incorrect. Full-disk Encryption doesn't only encrypt user directories; it encrypts the whole disk.

Option D is incorrect. Full-disk Encryption protects the data at all times, irrespective of the laptop's connection to a network.

Question 344. A large news website was rendered unavailable during a major news event. Network logs show an overwhelming amount of traffic from IoT devices. Which type of DDoS attack leveraged IoT devices is this indicative of?

- (A) Reflected Attack
- (B) **Botnet Attack**
- (C) Amplification Attack
- (D) Teardrop Attack

Explanation 344. Correct Answer: B. Botnet Attack. Botnets, which are networks of compromised devices (including IoT devices), are often used to conduct large-scale DDoS attacks by directing the combined bandwidth of the devices towards a target.

Option A is incorrect. In a reflected attack, an attacker sends traffic to a third party, disguising it as if it came from the victim,

which then reflects the traffic to the victim. It doesn't primarily involve IoT devices.

Option C is incorrect. An amplification attack leverages vulnerable network services to amplify the amount of traffic sent to a victim. The primary focus isn't the use of IoT devices.

Option D is incorrect. A teardrop attack involves sending mangled IP fragments with overlapping and oversized payloads to crash a target system. It doesn't specifically utilize IoT devices.

Question 345. A security administrator needs to apply a configuration change to a critical service, requiring a service restart. Before initiating the restart, which of the following steps is MOST important to ensure continuous service availability?

- (A) **Implement automatic service restart on failure**
- (B) Announce the restart to all company employees
- (C) Schedule the restart during off-peak hours
- (D) Take a backup of the current service configuration

Explanation 345. Correct Answer: A. Implement automatic service restart on failure. Having an automatic service restart on failure ensures that if any issues arise after applying the configuration change, the service will attempt to restart itself, ensuring minimal interruption to its availability.

Option B is incorrect. While notifying company employees is good practice, it doesn't directly ensure continuous service availability.

Option C is incorrect. Scheduling during off-peak hours minimizes impact but doesn't ensure the service will be available if issues arise post-restart.

Option D is incorrect. While taking a backup of the configuration is crucial for rollback purposes, it doesn't ensure the service will remain available immediately post-restart.

Question 346. The finance department at a large firm still relies on a legacy application for their quarterly reporting. This application is known to have some security flaws, but due to its critical nature, it cannot be easily replaced. How can the firm BEST mitigate the risks associated with this application?

- (A) Train the finance team about the latest cybersecurity threats
- (B) Run the legacy application on the latest hardware to improve performance
- (C) **Place the legacy application behind a web application firewall (WAF)**
- (D) Frequently change the passwords of users who have access to the application

Explanation 346. Correct Answer: C. Place the legacy application behind a web application firewall (WAF). By placing the application behind a WAF, the firm can filter, monitor, and block malicious HTTP traffic targeting the application's vulnerabilities, thereby offering a layer of protection against potential security flaws in the legacy application.

Option A is incorrect. While training is essential, it doesn't directly address the vulnerabilities in the legacy application.

Option B is incorrect. Using the latest hardware might improve application performance but doesn't mitigate the security risks associated with its vulnerabilities.

Option D is incorrect. While frequent password changes can enhance security, they don't address the inherent vulnerabilities in the legacy application.

Question 347. A company is preparing to roll out a new infrastructure deployment for its internal network. They have a server that will store both highly confidential customer information and non-sensitive marketing material. The IT department wants to ensure that only the confidential data is encrypted, while the marketing data remains easily accessible. Which level of encryption would be most suitable for this scenario?

- (A) File-level Encryption
- (B) Full-disk Encryption
- (C) **Partition Encryption**
- (D) Transport-layer Encryption

Explanation 347. Correct Answer: C. Partition Encryption. Partition Encryption allows specific partitions or volumes of a storage drive to be encrypted. By encrypting only the partition that contains confidential data, the company can ensure the security of sensitive information while leaving other partitions, such as the one with marketing material, unencrypted for easy access.

Option A is incorrect. File-level Encryption would require each confidential file to be encrypted individually, which could be cumbersome.

Option B is incorrect. Full-disk Encryption would encrypt the entire disk, including the non-sensitive marketing material.

Option D is incorrect. Transport-layer Encryption protects data in transit, not data at rest on storage drives

Question 348. An organization's security team discovered that an attacker had gained unauthorized access to a server. Upon investigating, they found a software tool that allowed the attacker to mask processes, files, and system data, effectively remaining hidden while maintaining privileged access. What type of malware was implanted by the attacker?

- (A) Trojan
- (B) Worm
- (C) Logic Bomb
- (D) **Rootkit**

Explanation 348. Correct Answer: D. Rootkit. A rootkit is malware that provides stealthy access to a computer and hides its presence from standard detection methods. It can mask files, processes, and other system data.

Option A is incorrect. A Trojan disguises itself as legitimate software but performs malicious activities once installed. It does not inherently hide processes or files.

Option B is incorrect. Worms are malware that can replicate themselves to spread to other systems. They don't typically hide their activities at the system level.

Option C is incorrect. A logic bomb is set to execute its malicious activity when a specific event or condition occurs. It doesn't focus on hiding system data or processes.

Question 349. As part of an initial penetration testing phase, Jackson is using tools that directly probe and interact with the target system's network to discover open ports, services, and other potential access points. While this approach is more direct and could be detected by the target's security systems, it provides detailed and actionable insights. Which type of reconnaissance is Jackson performing?

- (A) Threat analysis
- (B) Passive reconnaissance
- (C) **Active reconnaissance**
- (D) Social engineering

Explanation 349. Correct Answer: C. Active reconnaissance. Active reconnaissance involves directly interacting with the target systems to gain more detailed and actionable information. In this phase, tools and techniques that can be detected by the target's security measures, such as port scanning, are often used. Jackson's approach matches the characteristics of active reconnaissance.

Option A is incorrect. Threat analysis is the process of identifying, assessing, and prioritizing threats against a system or organization.

Option B is incorrect. Passive reconnaissance is about collecting data without direct interaction with the target systems, typically using third-party sources, public records, and other non-intrusive methods.

Option D is incorrect. Social engineering involves manipulating individuals to reveal confidential information or perform certain actions, and it is not directly related to network probing or service discovery.

Question 350. HealthCareNow, a large hospital chain, wants to ensure its newly implemented electronic health record (EHR) system adheres to national standards. Which type of audit would be most appropriate to confirm that HealthCareNow is in compliance with national regulations regarding patient data?

- (A) Self-assessment using internal standards
- (B) Third-party risk assessment
- (C) **External regulatory audit**
- (D) Informal peer review

Explanation 350. Correct Answer: C. External regulatory audit. External regulatory audits are conducted by external entities to ensure that organizations are complying with industry or national regulations. For HealthCareNow, an external regulatory audit will confirm that its EHR system complies with national standards related to patient data.

Option A is incorrect. While self-assessments are beneficial for internal reviews, they might not carry the same weight or depth of scrutiny that external regulatory audits possess.

Option B is incorrect. Third-party risk assessments focus on evaluating the security risks associated with external partners and vendors, not on confirming compliance with national regulations.

Option D is incorrect. An informal peer review might offer insights and suggestions but lacks the formal structure and regulatory emphasis of an external audit.

Question 351. A healthcare provider stores vast amounts of patient data on its servers. While they have strong perimeter defenses, they want an additional layer of security to ensure patient data remains confidential even in the event of unauthorized access. Which of the following would be the MOST effective solution for this requirement?

- (A) Use hash algorithms on all patient data
- (B) Implement data deduplication techniques
- (C) **Encrypt the stored patient data**
- (D) Use a web application firewall (WAF)

Explanation 351. Correct Answer: C. Encrypt the stored patient data. Encrypting patient data ensures that even if malicious actors gain access to the data, they won't be able to understand or utilize it without the proper decryption key.

Option A is incorrect. Hashing is primarily used for verifying data integrity or storing passwords securely. Hashing would not allow the healthcare provider to retrieve and use the patient data when needed.

Option B is incorrect. Data deduplication is about reducing storage requirements by removing duplicate data; it doesn't provide confidentiality.

Option D is incorrect. While a WAF provides protection against web-based threats, it doesn't ensure the confidentiality of stored data in the event of unauthorized access.

Question 352. John, a citizen of a country that strictly follows the General Data Protection Regulation (GDPR), used a global online shopping platform for a year. He decided to stop using the platform and requested the deletion of all his personal data. What is the online platform's primary obligation concerning John's request under the "Right to be Forgotten" principle?

- (A) Retain the data but ensure that John's data is never used for marketing purposes
- (B) Delete all personal data about John unless there's a legal reason to keep it**
- (C) Anonymize John's data and notify him of the completion
- (D) Move John's data to a secure, encrypted server where it won't be accessed

Explanation 352. Correct Answer: B. Delete all personal data about John unless there's a legal reason to keep it. The "Right to be Forgotten" under GDPR allows citizens to ask organizations to delete their personal data unless the organization has a legitimate reason (e.g., legal obligations) to retain the data.

Option A is incorrect. Merely refraining from using John’s data for marketing does not satisfy the “Right to be Forgotten.”

Option C is incorrect. Anonymization does not equate to the removal of data, and GDPR’s “Right to be Forgotten” specifically refers to the deletion of data.

Option D is incorrect. Simply moving the data to a secure server doesn’t align with the principles of the “Right to be Forgotten.” The data needs to be deleted unless there’s a valid reason to retain it.

Question 353. TechFirm, a leading technology conglomerate, recently conducted a security exercise. The goal was for the internal security team to defend against a series of simulated attacks from an external red team. While the red team launched attacks, the internal team’s objective was to detect, respond, and mitigate those threats. What type of penetration testing is TechFirm employing for its internal security team?

- (A) Offensive penetration testing
- (B) Passive penetration testing
- (C) **Defensive penetration testing**
- (D) Black box testing

Explanation 353. Correct Answer: C. Defensive penetration testing. Defensive penetration testing is designed to test the organization’s capability to defend its systems and networks against attacks. It typically involves an internal security team (often called the blue team) that defends against simulated attacks.

Option A is incorrect. Offensive penetration testing involves actively trying to exploit vulnerabilities, not defending against them.

Option B is incorrect. Passive penetration testing refers to gathering information without actively interacting with the target systems. It's not focused on defending against active threats.

Option D is incorrect. Black box testing is a method where the tester has no knowledge of the internal workings of the system they are testing. It doesn't describe a defensive posture.

Question 354. During a security assessment of an application, Ryan found that he was able to input larger-than-expected data into a field. Upon doing so, he noticed the application became unresponsive and eventually crashed. What type of vulnerability might Ryan have uncovered?

- (A) Input Validation Error
- (B) Cross-Site Scripting (XSS)
- (C) **Buffer Overflow**
- (D) Insecure Direct Object Reference (IDOR)

Explanation 354. Correct Answer: C. Buffer Overflow.

Buffer overflow vulnerabilities occur when an application allows more input data than it can securely handle in its allocated buffer space, leading to overwritten adjacent memory. This can lead to application crashes, or potentially, arbitrary code execution by an attacker.

Option A is incorrect. While input validation error can lead to various vulnerabilities, it is a broad category. In the given scenario, the direct consequence of entering larger than expected data is an application crash, which points directly to a buffer overflow.

Option B is incorrect. Cross-Site Scripting (XSS) vulnerabilities allow attackers to inject malicious scripts into web pages viewed by other users. It doesn't cause application crashes due to oversized input.

Option D is incorrect. Insecure Direct Object Reference (IDOR) vulnerabilities occur when an application provides direct access to objects based on user input. It does not cause crashes due to excessive data input.

Question 355. A financial institution wants to ensure that if a cyber attacker gains unauthorized access to one section of their network, the attacker cannot easily move laterally to more sensitive parts of the network. Which method can help achieve this objective?

- (A) Deploying a honeypot in every segment
- (B) **Implementing network segmentation**
- (C) Applying encryption on all data traffic
- (D) Enabling two-factor authentication for all users

Explanation 355. Correct Answer: B. Implementing network segmentation. Network segmentation divides a network into multiple segments or subnets. Each segment operates independently and can have its own security and access

controls. This means that if an attacker compromises one segment, they won't necessarily have access to other segments.

Option A is incorrect. A honeypot is a decoy system to attract potential attackers, but it doesn't prevent lateral movement within the network once an attacker has access.

Option C is incorrect. While encrypting data traffic ensures confidentiality, it doesn't prevent lateral movement within the network.

Option D is incorrect. Two-factor authentication strengthens access controls but doesn't inherently stop lateral movement within a network if an attacker gains access.

Question 356. Emily, an executive assistant, receives a phone call from an individual claiming to be a new employee in the IT department. The caller says they're conducting a routine check and needs Emily to confirm her username and password for system verification. How should Emily respond?

- (A) **Politely decline and report the call to the IT department**
- (B) Provide the caller with the username but not the password
- (C) Ask the caller to email the request, so there's a written record
- (D) Hang up without saying anything

Explanation 356. Correct Answer: A. Politely decline and report the call to the IT department. This is a classic example of a vishing (voice phishing) attempt, a form of social

engineering. The best practice in such scenarios is to never provide sensitive information over the phone, especially when the call is unsolicited. Reporting the attempt to the IT department can help the company be aware and potentially prevent further attempts.

Option B is incorrect. Even if Emily provides only her username, it could still be used maliciously in combination with other attacks.

Option C is incorrect. Written records can be helpful, but it's crucial not to entertain or validate unsolicited requests, whether via email or phone.

Option D is incorrect. While hanging up stops the immediate threat, it's essential to report such incidents for broader organizational awareness and protection.

Question 357. SafeNet, a financial institution, decided to undertake a comprehensive security assessment. They brought together their internal security team and an external group of ethical hackers. Their objective was for these teams to collaboratively assess vulnerabilities, perform real-time attack simulations, and evaluate defense mechanisms. What form of penetration testing is SafeNet utilizing?

- (A) Black box testing
- (B) **Integrated penetration testing**
- (C) Defensive penetration testing
- (D) Red team assessment

Explanation 357. Correct Answer: B. Integrated penetration testing. Integrated penetration testing, often associated with purple teaming, involves the combined efforts of both offensive and defensive teams to provide a holistic assessment of an organization's security posture.

Option A is incorrect. Black box testing is a method where the tester doesn't have prior knowledge of the system's architecture or underlying code. It doesn't emphasize the collaborative nature between offensive and defensive teams.

Option C is incorrect. Defensive penetration testing focuses on evaluating the defensive capabilities of an organization against potential attacks, without necessarily implying collaboration with an offensive team.

Option D is incorrect. Red team assessment involves simulating real-world cyber-attacks to test an organization's security posture, but it doesn't inherently suggest a joint effort with a defensive team.

Question 358. A company's proprietary algorithm is being targeted by competitors aiming to replicate its functionality. To safeguard its intellectual property without changing the algorithm's behavior, the company wants a method that disguises the original code structure. What should they implement?

- (A) Data masking on the algorithm's output
- (B) **Obfuscation on the algorithm's code**
- (C) Encryption of the algorithm's storage location

(D) Implementing a hashing mechanism within the algorithm

Explanation 358. Correct Answer: B. Obfuscation on the algorithm's code. Obfuscating the algorithm's code will make it more challenging to understand, reverse engineer, or replicate, without altering its behavior or results.

Option A is incorrect. Data masking on the algorithm's output would only hide or change certain parts of the output. It doesn't protect or disguise the algorithm's actual code or logic.

Option C is incorrect. Encrypting the algorithm's storage location protects the stored data from unauthorized access, but once accessed (e.g., for legitimate use), the original code structure would still be visible.

Option D is incorrect. Implementing a hashing mechanism within the algorithm might change its behavior and doesn't obscure the algorithm's logic or structure.

Question 359. AlphaTech, a leading tech manufacturer, is considering a penetration test to identify vulnerabilities in their new product's firmware. They provide the testers with firmware source code, architecture diagrams, and other internal details to ensure a thorough evaluation. What kind of penetration test is AlphaTech commissioning?

- (A) Zero-knowledge testing
- (B) **Open box testing**
- (C) Opaque testing
- (D) Blind testing

Explanation 359. Correct Answer: B. Open box testing.

Open box testing, similar to white box testing, is where the tester is given complete transparency and full details about the system internals, making it easier to identify vulnerabilities that might be missed in other forms of testing.

Option A is incorrect. Zero-knowledge testing is another term for black box testing, where testers have no knowledge of the system internals.

Option C is incorrect. Opaque testing is not a recognized term in penetration testing methodologies and is intended as a distractor.

Option D is incorrect. Blind testing is a scenario where the testers have limited knowledge about the target system.

Question 360. Lisa, a cybersecurity analyst, is setting up a centralized system to correlate logs from multiple sources, detect malicious activities in real-time, and produce comprehensive security reports. Which tool should Lisa consider for this purpose?

- (A) Network Intrusion Detection System (NIDS)
- (B) Web Application Firewall (WAF)
- (C) Vulnerability Scanner
- (D) **Security Information and Event Management (SIEM)**

Explanation 360. Correct Answer: D. Security Information and Event Management (SIEM). SIEM tools are designed to aggregate, correlate, and analyze logs and events from various

sources in an organization. They help in detecting and responding to security incidents in real-time and generating detailed security reports.

Option A is incorrect. While NIDS monitors and analyzes network traffic for signs of malicious activities, it doesn't provide centralized logging and reporting functionalities like a SIEM.

Option B is incorrect. A Web Application Firewall (WAF) protects web applications from web-based attacks. It does not offer the centralized log correlation and analysis features of a SIEM.

Option C is incorrect. A Vulnerability Scanner identifies vulnerabilities in systems and applications but doesn't aggregate and analyze logs from various sources.

Question 361. WebMasters LLC, a popular web hosting company, wants to ensure the robust security of their hosted websites. They initiate a security challenge, inviting ethical hackers worldwide to find vulnerabilities without giving any details about their servers, databases, or applications. Which penetration testing method is WebMasters LLC utilizing?

- (A) External testing
- (B) Grey box testing
- (C) Active testing
- (D) **Black box testing**

Explanation 361. Correct Answer: D. Black box testing. In black box testing, the testers are not provided with any

knowledge about the system's internals and have to identify vulnerabilities based purely on their own discoveries.

WebMasters LLC's approach, where they don't disclose any specifics to the ethical hackers, resonates with this method.

Option A is incorrect. While the challenge by WebMasters LLC can be externally focused, external testing alone doesn't define the level of knowledge provided to the testers.

Option B is incorrect. In grey box testing, testers would have some knowledge about the target, which is not the case here.

Option C is incorrect. Active testing simply means testers are directly interacting with the system, but it doesn't specify the amount of knowledge they have about its internals.

Question 362. After an annual review, BestTech Co. realized that their IT team was unfamiliar with the protocols to follow during a data breach. To ensure the team understands the steps and decision points without launching a live drill, what should the company implement?

- (A) Upgrade their firewall systems
- (B) **Engage in a tabletop exercise**
- (C) Conduct a red team exercise
- (D) Implement multi-factor authentication for all users

Explanation 62. Correct Answer: B. Engage in a tabletop exercise. Tabletop exercises allow teams to discuss and review specific scenarios, such as a data breach, and ensure everyone understands their roles and the processes to follow. It's a cost-effective way to familiarize the team with response procedures.

Option A is incorrect. Upgrading firewall systems may enhance the company's security posture but doesn't familiarize the IT team with data breach response protocols.

Option C is incorrect. A red team exercise is a live simulated attack to evaluate the organization's security posture and does not focus on walking the team through the response steps in a controlled environment.

Option D is incorrect. Multi-factor authentication is a security measure to validate users' identities but does not address the team's unfamiliarity with data breach response protocols.

Question 363. A medium-sized organization recently had a third-party auditor review their information security controls. After the review, the auditor provided a formal statement that verified the effectiveness of the controls in place. What is this formal statement referred to as?

- (A) Certification
- (B) Accreditation
- (C) **Attestation**
- (D) Assurance

Explanation 363. Correct Answer: C. Attestation. An attestation is a formal statement or declaration by a subject matter expert, like an auditor, attesting that specific criteria are met. In this case, the auditor is attesting to the effectiveness of the information security controls.

Option A is incorrect. Certification is the process of providing someone or something with an official document attesting to a

status or level of achievement, which may or may not involve testing against certain standards.

Option B is incorrect. Accreditation is the formal recognition that a body or individual is competent to perform specific tasks, usually granted by a higher authority or body.

Option D is incorrect. Assurance refers to the measures taken to gain confidence in the security of a system, but it's not a formal declaration like an attestation.

Question 364. In preparation for an upcoming audit, AlphaTech Corporation hires a team to evaluate their security measures. The team is spotted attempting to bypass security barriers, unlock doors without keys, and trying to access restricted floors by pretending to be maintenance staff. What type of testing is AlphaTech Corporation undergoing?

- (A) Network vulnerability scanning
- (B) **Physical penetration testing**
- (C) OS fingerprinting
- (D) Source code review

Explanation 364. Correct Answer: B. Physical penetration testing. Physical penetration testing involves hands-on techniques to breach physical barriers, such as locks, security checkpoints, or restricted areas, to assess the efficacy of physical security controls.

Option A is incorrect. Network vulnerability scanning is about identifying vulnerabilities in networked systems through automated tools, not physical barriers.

Option C is incorrect. OS fingerprinting identifies the operating system of a remote computer. It doesn't involve physically trying to access restricted areas.

Option D is incorrect. Source code review evaluates the source code of applications for vulnerabilities and doesn't concern physical access controls.

Question 365.. WebSoft Inc., a leading software company, recently launched a new web application. Before making it live, they engaged a security firm to challenge the application, find vulnerabilities, and exploit them as real hackers would. This aggressive testing is done to ensure maximum security. What kind of penetration testing is WebSoft Inc. opting for?

- (A) White box testing
- (B) Defensive penetration testing
- (C) **Offensive penetration testing**
- (D) Gray box testing

Explanation 365. Correct Answer: C. Offensive penetration testing. Offensive penetration testing is an aggressive form of testing where the tester actively attempts to find and exploit vulnerabilities in the target system or application, much like a real attacker.

Option A is incorrect. White box testing, also known as clear box testing, involves having full visibility and knowledge of the internal workings of the application being tested. The focus is more on the methodology and not the aggressive nature of the testing.

Option B is incorrect. There is no specific testing method called “defensive penetration testing.” Defensive strategies are typically associated with blue team activities that focus on defending systems, not aggressively testing them.

Option D is incorrect. Gray box testing is a combination of both white box and black box testing methods. Testers have some knowledge of the internal workings but not complete information. The emphasis here is on the level of knowledge of the system and not on the aggressive nature of the testing.

Question 366. After a series of high-profile data breaches in the industry, OnlineRetail Corp., an e-commerce platform, wishes to undergo an external review to validate the security of its operations and provide a comprehensive report to its shareholders. Which type of assessment will provide a detailed and formalized examination of their security posture?

- (A) **External examination of IT controls and operations**
- (B) Internal review of security protocols
- (C) External regulatory audit on financial statements
- (D) Informal feedback from industry peers

Explanation 366. Correct Answer: A. External examination of IT controls and operations. An external examination of IT controls and operations provides a deep and structured assessment of an organization’s security posture and IT operations. Conducted by external experts, it can provide formalized, comprehensive findings to reassure shareholders of the company’s security measures.

Option B is incorrect. An internal review is conducted by the organization's own personnel and may lack the independent perspective and comprehensive scope of an external examination.

Option C is incorrect. An external regulatory audit on financial statements focuses on financial reporting and not on the security of IT operations.

Option D is incorrect. Informal feedback, while potentially useful, does not offer the structured, comprehensive, and independent insights that an external examination provides.

Question 367. XYZ Ltd. wants to evaluate if their current security measures are consistent with industry-specific regulations they are required to follow. The evaluation should be done by their own IT department before inviting external auditors. Which approach should XYZ Ltd. adopt?

- (A) Third-party vulnerability scanning
- (B) **Internal compliance assessment**
- (C) External attestation
- (D) Vendor risk assessment

Explanation 367. Correct Answer: B. Internal compliance assessment. An internal compliance assessment is conducted by an organization's internal teams to evaluate if their operations, processes, and configurations are in alignment with required compliance standards or regulations. This helps in proactively identifying and rectifying non-compliance before an external audit.

Option A is incorrect. Third-party vulnerability scanning focuses on identifying vulnerabilities and doesn't necessarily check for compliance with industry-specific regulations.

Option C is incorrect. External attestation is a formal statement from an external party verifying specific criteria. This would not be done by the company's internal IT department.

Option D is incorrect. Vendor risk assessment focuses on assessing the security risks associated with third-party vendors and doesn't evaluate an organization's internal compliance with regulations.

Question 368. SafeNet Banking Corporation is keen on gaining a competitive edge in the market by demonstrating its commitment to cybersecurity. They want an official attestation that their cybersecurity measures are robust and compliant with industry standards. What should SafeNet opt for to obtain this attestation?

- (A) Feedback from customers on the bank's app security
- (B) Internal IT team's report on cybersecurity practices
- (C) **External independent third-party audit**
- (D) Informal evaluation by a cybersecurity consultancy

Explanation 368. Correct Answer: C. External independent third-party audit. An external independent third-party audit can provide an official attestation regarding SafeNet Banking Corporation's adherence to industry standards in cybersecurity. By having an external entity evaluate their practices, SafeNet can assure stakeholders of its commitment to cybersecurity.

Option A is incorrect. While feedback from customers is valuable, it is not an official or comprehensive assessment of the bank's entire cybersecurity practices.

Option B is incorrect. An internal IT team's report might lack the external perspective and official attestation that a third-party audit can provide.

Option D is incorrect. An informal evaluation, even by a cybersecurity consultancy, might not be as rigorous or recognized as an official third-party audit.

Question 369. The company's security administrator observes that there are multiple unauthorized access attempts originating from IP addresses in a specific range. The administrator wants to prevent these IP addresses from accessing the corporate network temporarily. Which of the following firewall configurations would BEST address this requirement?

- (A) **Configure an implicit deny rule for the specific IP range**
- (B) Set up a honeypot for the specific IP range
- (C) Allow the IP range but set a bandwidth limit
- (D) Add the IP range to a whitelist

Explanation 369. Correct Answer: A. Configure an implicit deny rule for the specific IP range. By configuring an implicit deny rule for that specific IP range, the firewall will block any traffic from those addresses, preventing them from accessing the network.

Option B is incorrect. While a honeypot can be used to monitor and analyze attacker behavior, it does not block the access of the specified IP range to the corporate network.

Option C is incorrect. Allowing the IP range and setting a bandwidth limit would not prevent access; it would only restrict the amount of data they could send/receive.

Option D is incorrect. Adding the IP range to a whitelist would grant them access, which is opposite to the required action.

Question 370. Lisa, a security administrator, is using a popular benchmark to ensure the web servers in her organization are configured securely. She wants to make sure that unnecessary services are disabled, and appropriate permissions are set. Which of the following organizations is MOST likely the source of the benchmark she is using?

- (A) PCI DSS
- (B) OWASP
- (C) CIS
- (D) GDPR

Explanation 370. Correct Answer: C. CIS. The Center for Internet Security (CIS) is known for its CIS Benchmarks, which provide prescriptive guidance for configuring systems securely.

Option A is incorrect. PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

Option B is incorrect. OWASP (Open Web Application Security Project) is known for its top ten list of web application vulnerabilities and not for system configuration benchmarks.

Option D is incorrect. GDPR (General Data Protection Regulation) is a regulation that requires businesses to protect the personal data and privacy of EU citizens. It doesn't provide benchmarks for secure system configurations.

Question 371. ZenTech, a multinational corporation, recently adopted a multi-cloud strategy, deploying workloads across multiple cloud service providers. What is a primary security benefit of this approach?

- (A) Centralized management of all cloud resources
- (B) Automatic encryption of data in transit between clouds
- (C) **Mitigation against a single point of failure**
- (D) Reduction in the cost of cloud storage solutions

Explanation 371. Correct Answer: C. Mitigation against a single point of failure. Using a multi-cloud strategy distributes workloads across various cloud providers, which reduces the risk associated with outages or security breaches in any one provider. This diversification ensures that a failure or compromise in one cloud environment doesn't jeopardize the entire infrastructure.

Option A is incorrect. Multi-cloud strategies can sometimes complicate management due to the need to interface with different platforms and providers. Centralization isn't the primary benefit in this context.

Option B is incorrect. While encryption is crucial, adopting a multi-cloud approach doesn't automatically encrypt data in transit between different cloud environments. This would require specific configurations and solutions.

Option D is incorrect. While cost optimization can be a factor in adopting a multi-cloud strategy, the primary security advantage is not related to cost reduction.

Question 372. A company wants to host a public-facing website but ensure that even if the website gets compromised, attackers cannot gain access to sensitive internal data. Which of the following is the BEST configuration to achieve this?

- (A) Place the web server on the internal network and strictly monitor the traffic
- (B) Place the web server in the DMZ with a firewall in front of it and another firewall between the DMZ and the internal network**
- (C) Directly connect the web server to the internet without a firewall and move sensitive data off the server
- (D) Place the web server in the DMZ and connect it directly to the internal network without a firewall

Explanation 372. Correct Answer: B. Place the web server in the DMZ with a firewall in front of it and another firewall between the DMZ and the internal network. By placing the web server in a DMZ, and having two firewalls (one facing the internet and another facing the internal network), the company can ensure that even if the public-facing web server is compromised, the attacker would still need to bypass another firewall to reach the internal network.

Option A is incorrect. Placing a public-facing web server on the internal network, even with monitoring, exposes the network to unnecessary risks.

Option C is incorrect. Connecting a server directly to the internet without any form of firewall is highly risky, even if sensitive data is moved.

Option D is incorrect. Without a firewall between the DMZ and the internal network, it becomes much easier for a compromised server in the DMZ to impact or access the internal network.

Question 373. TechFirm Inc. collects personal data from its users and decides on the purposes and means of processing this data. They also outsource data storage to CloudData, a third-party company. In the context of data privacy regulations, how would TechFirm and CloudData be classified respectively?

- ((A) TechFirm: Processor; CloudData: Controller
- (B) TechFirm: Controller; CloudData: Processor**
- (C) Both TechFirm and CloudData: Processors
- (D) Both TechFirm and CloudData: Controllers

Explanation 373. Correct Answer: B. TechFirm: Controller; CloudData: Processor. TechFirm Inc., which decides on the purposes and means of processing personal data, is the “Controller”. CloudData, which is responsible for processing data on behalf of TechFirm (without deciding on its use), is the “Processor”.

Option A is incorrect. The roles are reversed in this option. TechFirm is the one making decisions on data use, so it's the Controller.

Option C is incorrect. Both entities have different roles in this scenario. TechFirm is not just processing; it's deciding on how the data should be used, making it a Controller.

Option D is incorrect. CloudData does not decide on the purpose and means of the data processing. It simply processes data on behalf of TechFirm, making it a Processor.

Question 374. The IT department of Globex Corp is concerned about the increasing number of malicious websites being accessed from company laptops while employees are working remotely. They want to ensure that the web filter policies set in the corporate network are enforced even when devices are offsite. What would be the BEST solution to address this concern?

- (A) Implement a cloud-based web filtering solution
- (B) Use a VPN to force all remote traffic through the corporate network
- (C) **Deploy an agent-based web filter on all company laptops**
- (D) Periodically send reminders to employees about acceptable web usage

Explanation 374. Correct Answer: C. Deploy an agent-based web filter on all company laptops. Agent-based web filters can enforce web filtering policies on a device regardless of its

location. This ensures that the policies apply consistently whether the device is on or off the corporate network.

Option A is incorrect. While cloud-based solutions can offer offsite filtering, they might not be as consistent as an agent-based solution that directly enforces corporate policies on the device itself.

Option B is incorrect. Using a VPN would force all traffic through the corporate network, which could cause latency and might not be feasible for all remote work scenarios.

Option D is incorrect. Sending reminders is a passive approach and may not effectively prevent access to malicious websites.

Question 375. SoftTech Solutions is a software development company that has decided to conduct a penetration test on their new web application. The testers are provided with user credentials, network topology diagrams, and some proprietary software code snippets. Which type of penetration testing is SoftTech Solutions employing?

- (A) Black box testing
- (B) Double-blind testing
- (C) **Known environment testing**
- (D) Zero-knowledge testing

Explanation 375. Correct Answer: C. Known environment testing. Known environment testing is a type of penetration testing where the testers are given certain information about the target's environment. This can include user credentials, network

diagrams, and more, to mimic a potential insider threat or a threat actor who has gained certain internal information.

Option A is incorrect. In black box testing, testers are given no prior knowledge about the system.

Option B is incorrect. In double-blind testing, neither the attackers nor the defenders have prior knowledge of the impending test.

Option D is incorrect. Zero-knowledge testing is another term for black box testing, where the testers have no knowledge of the system internals.

Question 376. DeltaTech, a financial institution, operates its primary site on a UNIX-based platform. For disaster recovery purposes, they are considering setting up a backup site on a different platform. Which of the following is NOT a primary benefit of introducing platform diversity in this case?

- (A) **It reduces the organization's learning curve by using familiar technologies**
- (B) It provides resilience against attacks targeting UNIX-based systems
- (C) It ensures that platform-specific outages don't affect both primary and backup sites
- (D) It diversifies the attack surface, reducing the impact of specific platform vulnerabilities

Explanation 376. Correct Answer: A. It reduces the organization's learning curve by using familiar technologies. Introducing a new platform usually increases the learning curve

as staff need to be trained on the new system. The primary benefits of platform diversity are resilience, redundancy, and diversifying the attack surface.

Option B is incorrect. This is one of the benefits of platform diversity. If a vulnerability or threat targets UNIX-based systems, having a backup on a different platform ensures that the backup isn't compromised by the same threat.

Option C is incorrect. This is a benefit of platform diversity. Platform-specific outages or issues would only affect systems on that platform, so having a backup on a different platform adds resilience.

Question 377. After a recent security incident, Sarah, a network security analyst, wants to analyze the flow data of network traffic to identify patterns and potential threats. She wants to collect metadata about IP traffic flow and gather details like IP addresses, ports, and protocols used. Which tool should Sarah employ to obtain this information?

- (A) Intrusion Detection System (IDS)
- (B) Syslog server
- (C) **NetFlow collector**
- (D) Simple Network Management Protocol (SNMP) traps

Explanation 377. Correct Answer: C. NetFlow collector.

NetFlow is a network protocol developed by Cisco for collecting IP traffic information and monitoring network traffic. A NetFlow collector can provide insights into traffic flow patterns and volume, making it suitable for Sarah's requirements.

Option A is incorrect. While an IDS can provide alerts on malicious activities based on specific signatures or heuristics, it does not provide detailed flow data analysis like NetFlow.

Option B is incorrect. A Syslog server is mainly used for collecting and storing log data from various devices. It does not focus on detailed network traffic flow like NetFlow.

Option D is incorrect. SNMP traps are for sending unsolicited alert messages from a device to a management station regarding specific events. They don't provide traffic flow analysis.

Question 378. A large financial institution recently experienced a security breach where an attacker was able to bypass its intrusion detection system (IDS). Upon investigation, the security team found out that the attacker utilized a zero-day exploit. In the aftermath, what should the institution do to enhance the capability of its IDS?

- (A) **Switch from a signature-based IDS to a behavior-based IDS**
- (B) Disable the IDS and rely solely on firewall rules
- (C) Update the IDS with the latest threat intelligence feeds and signatures
- (D) Reduce the frequency of IDS signature updates

Explanation 378. Correct Answer: A. Switch from a signature-based IDS to a behavior-based IDS. Behavior-based IDS (or anomaly-based IDS) monitors network traffic and compares it against an established baseline, allowing it to potentially detect zero-day exploits and other novel attacks that signature-based systems might miss.

Option B is incorrect. Relying solely on firewall rules without IDS would lessen the security depth and expose the institution to more risks.

Option C is incorrect. While updating the IDS with the latest signatures is important, it wouldn't necessarily detect zero-day exploits until a signature for that exploit has been created and disseminated.

Option D is incorrect. Reducing the frequency of IDS signature updates would make the system even more vulnerable to recent threats.

Question 379. After a major power outage, TechWave Corp. wants to ensure their primary data center's operations can be swiftly and seamlessly shifted to another facility. The company wants this process to be automated and immediate to prevent any service interruption. What type of test should TechWave Corp. conduct to validate this functionality?

- (A) Conduct a vulnerability assessment on both data centers
- (B) **Execute a failover test**
- (C) Engage in a tabletop exercise
- (D) Perform a routine backup test

Explanation 379. Correct Answer: B. Execute a failover test.

A failover test involves simulating a failure in the primary system to ensure that the backup system can seamlessly take over without any service interruption. It helps in verifying the resilience and recovery capabilities of an organization's infrastructure.

Option A is incorrect. A vulnerability assessment identifies potential weaknesses in systems but does not test the seamless transition between primary and backup systems.

Option C is incorrect. A tabletop exercise is a discussion-based session and does not involve the live testing of systems or processes.

Option D is incorrect. A routine backup test ensures that backups can be restored successfully but does not test the immediate switchover capability between systems.

Question 380. Sarah, a security administrator, is implementing a monitoring solution for her organization's server infrastructure. She wants a solution that does not require any additional software to be installed on the servers themselves. Which type of monitoring approach should Sarah choose?

- (A) Agent-based monitoring
- (B) Intrusion Detection System (IDS)
- (C) **Agentless monitoring**
- (D) Network-based Application Performance Monitoring (APM)

Explanation 380. Correct Answer: C. Agentless monitoring.

Agentless monitoring solutions do not require any software agents to be installed on the servers they monitor. They typically rely on standard protocols and interfaces to collect performance and other data.

Option A is incorrect. Agent-based monitoring requires the installation of software agents on each server or device that is to be monitored.

Option B is incorrect. While an Intrusion Detection System (IDS) is a security tool, it is not specifically designed for agentless infrastructure monitoring.

Option D is incorrect. Network-based Application Performance Monitoring (APM) is focused on monitoring application performance on the network, not on agentless server monitoring.

Question 381. Alice, a cybersecurity analyst, is tasked with identifying potential weaknesses in a newly deployed web application's infrastructure before it goes live. She wants a tool that can proactively discover and report on system vulnerabilities, missing patches, and misconfigurations. Which of the following should Alice utilize for this purpose?

- (A) Intrusion Detection System (IDS)
- (B) Network sniffer
- (C) **Vulnerability scanner**
- (D) Security Information and Event Management (SIEM) system.

Explanation 381. Correct Answer: C. Vulnerability scanner.

Vulnerability scanners are designed to discover and report potential vulnerabilities in systems by probing and analyzing them. They can detect issues such as missing patches, misconfigurations, and known software flaws.

Option A is incorrect. An IDS detects and alerts on potential malicious activities based on specific signatures or heuristics but does not proactively scan for vulnerabilities.

Option B is incorrect. A network sniffer captures and analyzes network traffic but does not perform vulnerability assessments on infrastructure components.

Option D is incorrect. While a SIEM system can aggregate and analyze log and event data from various sources, it does not proactively scan for vulnerabilities like a vulnerability scanner

Question 382. After conducting a business impact analysis, a local library determined that they could afford several days of downtime without a significant impact on their operations. They want a disaster recovery solution that offers a balance between cost and recovery capabilities. Which site consideration is the most suitable for the library's needs?

- (A) Mobile site with a full set of IT equipment
- (B) Hot site with daily data replication
- (C) **Cold site**
- (D) Warm site with weekly backups

Explanation 382. Correct Answer: C. Cold site. A cold site is an offsite facility that is pre-configured to accept equipment and data backups but doesn't have any of its own. Given the library's tolerance for several days of downtime, a cold site would be a cost-effective solution that aligns with their recovery capabilities.

Option A is incorrect. A mobile site with a full set of IT equipment would be more suitable for immediate recovery needs and might be overkill for a library that can tolerate several days of downtime.

Option B is incorrect. A hot site with daily data replication would be more suited for businesses with a low tolerance for downtime and would likely be more expensive than the library's budget allows.

Option D is incorrect. Even though a warm site with weekly backups might seem like a viable option, a cold site would still be more cost-effective for the library given their tolerance for downtime.

Question 383. After a recent security incident in the organization, the IT team noticed that several legitimate activities were being flagged by the intrusion detection system, resulting in a high number of false positives. What is the MOST appropriate action to improve the system's accuracy and reduce unnecessary alerts?

- (A) Disable the intrusion detection system for a week to observe regular network traffic patterns
- (B) Set up a stricter firewall rule to block all external traffic
- (C) **Implement alert tuning to refine the system's detection criteria**
- (D) Encourage employees to reduce their internet usage

Explanation 383. Correct Answer: C. Implement alert tuning to refine the system's detection criteria. Alert tuning involves adjusting the detection rules or criteria of a system to

better differentiate between legitimate and malicious activities, thereby reducing false positives.

Option A is incorrect. Disabling the intrusion detection system can expose the organization to real threats, making it a risky approach.

Option B is incorrect. Setting up stricter firewall rules doesn't directly address the issue of false positives from the intrusion detection system and could block legitimate business operations.

Option D is incorrect. Reducing internet usage does not necessarily correlate with a decrease in false positives. The issue lies with the system's criteria, not the amount of traffic.

Question 384. Amy, a network administrator, is researching tools to assist with automating the evaluation of her organization's systems against a specific security baseline. She comes across SCAP and wants to implement it. Which of the following BEST describes the primary function of the Security Content Automation Protocol (SCAP)?

Content Automation Protocol (SCAP)?

(A) To facilitate the real-time transfer of threat intelligence feeds

(B) To provide an interface for user authentication against Active Directory

(C) **To allow for automated vulnerability management and policy compliance evaluation**

(D) To offer encrypted communication channels for remote system management

Explanation 384. Correct Answer: C. To allow for automated vulnerability management and policy compliance evaluation. SCAP (Security Content Automation Protocol) is a suite of open standards that enhances the ability of organizations to automate vulnerability management, measurement, and policy compliance evaluation on systems.

Option A is incorrect. While threat intelligence is crucial for security, SCAP is not designed primarily for real-time threat intelligence feed transfers.

Option B is incorrect. SCAP does not directly deal with user authentication against any directory services.

Option D is incorrect. SCAP's primary function isn't to offer encrypted communication channels for remote system management. Other protocols and tools serve this purpose.

Question 385. A financial institution wants to ensure that any unauthorized access to customer data triggers an immediate alert to the security team. Which of the following approaches would be the MOST effective in achieving this requirement?

- (A) Configure alerts for any modification to database records
- (B) Set up alerts for successful logins during off-business hours
- (C) **Establish alerting thresholds based on anomalous user behavior**
- (D) Send daily reports of all access attempts to the security team for review

Explanation 385. Correct Answer: C. Establish alerting thresholds based on anomalous user behavior. By setting alerting thresholds based on anomalous behavior, the system can detect unauthorized access based on patterns that deviate from typical user behavior, providing timely alerts for potential breaches.

Option A is incorrect. Configuring alerts for any modification to database records may generate a high number of false positives, especially in a dynamic environment like a financial institution where legitimate changes occur regularly.

Option B is incorrect. While setting up alerts for off-hours access can catch some unauthorized attempts, it might miss breaches occurring during business hours.

Option D is incorrect. Daily reports may delay the detection and response to unauthorized access, as it doesn't offer real-time alerting.

Question 386. After the recent cyber-attack on Acme Corp, the IT security team decided to enhance their proactive defense mechanism. They want to start with identifying unpatched and vulnerable systems on their network. Which of the following scanning activities would BEST assist them in this endeavor?

- (A) Conducting a passive scan during business hours
- (B) Implementing a full open port scan on all systems
- (C) **Running a credentialed vulnerability scan on their network**
- (D) Scanning the external perimeter for domain name resolutions

Explanation 386. Correct Answer: C. Running a credentialed vulnerability scan on their network. A credentialed vulnerability scan uses valid user credentials to access and scan the target system, allowing for a deeper and more comprehensive check for vulnerabilities, including unpatched systems.

Option A is incorrect. A passive scan is non-intrusive and only monitors network traffic, limiting its capability to identify unpatched systems actively.

Option B is incorrect. While a full open port scan can identify open ports, it doesn't necessarily identify unpatched systems or specific vulnerabilities.

Option D is incorrect. Scanning the external perimeter for domain name resolutions can help in gathering information about domain names but won't directly assist in identifying unpatched systems.

Question 387. A healthcare provider wants to evaluate the security of their patient portal. They inform the penetration testers about the technologies used, such as the programming languages and databases. However, specifics about the security measures in place, including intrusion detection systems, are kept secret. What kind of penetration test are they aiming for?

- (A) White box testing
- (B) External testing
- (C) **Grey box testing**
- (D) Active testing

Explanation 387. Correct Answer: C. Grey box testing. Grey box testing implies that testers have some knowledge about the target but not all details. Here, the healthcare provider gives details about the technologies used but keeps information about the security measures a secret. This partial disclosure aligns with grey box testing methodology.

Option A is incorrect. In white box testing, testers would have a complete overview of the system, including its code, configurations, and security measures.

Option B is incorrect. External testing primarily focuses on the system's exterior defenses, like firewall configurations, without consideration of what details are shared with the testers.

Option D is incorrect. Active testing means testers are directly interacting with the system and is not indicative of the level of knowledge they possess about the system's internals.

Question 388. Sarah, a sales manager at TechWorld Inc., receives an email from her bank urging her to update her account details due to a recent security breach. The email provides a link to a website that looks almost identical to her bank's official site. However, she notices a slight misspelling in the URL. What should Sarah do next?

- (A) Forward the email to her colleagues as a warning
- (B) Click the link and update her details as the bank's site is probably just undergoing updates
- (C) Delete the email without taking any action
- (D) **Report the email to her company's IT department and avoid clicking any links**

Explanation 388. Correct Answer: D. Report the email to her company's IT department and avoid clicking any links.

Sarah likely received a phishing email, a common tactic used by attackers to deceive users into providing sensitive information. The best course of action is to report the suspicious email to the IT department so they can take necessary precautions and notify other employees.

Option A is incorrect. While Sarah has the right instinct to warn others, forwarding potentially malicious emails can lead to more risks. It's better to alert the IT department.

Option B is incorrect. Clicking on links in suspicious emails, especially with a misspelled URL, can lead to compromised personal and company data.

Option C is incorrect. Simply deleting the email doesn't address the broader risk to the organization. Reporting such incidents helps the company bolster its defenses.

Question 389. Paul, a network administrator, has configured various networking devices in his organization to send alerts in the event of specific failures. After a switch experienced a power supply failure, Paul received an immediate notification. Which of the following did Paul most likely utilize to receive this notification?

- (A) Syslog server
- (B) **Simple Network Management Protocol (SNMP) traps**
- (C) Packet sniffer
- (D) Firewall logs

Explanation 389. Correct Answer: B. Simple Network Management Protocol (SNMP) traps. SNMP traps are unsolicited alert messages sent by a device to notify an SNMP management station of specific events. In this case, the switch sent an SNMP trap to Paul when it detected the power supply failure.

Option A is incorrect. While a Syslog server can be used to collect logs from various devices, it doesn't proactively send alerts based on specific events like an SNMP trap does.

Option C is incorrect. A packet sniffer captures and analyzes network traffic but doesn't actively alert administrators to specific device events.

Option D is incorrect. Firewall logs are specific to firewalls and track traffic that passes through the firewall, but they don't typically send unsolicited alerts about network device health.

Question 390. Samantha, a security analyst, has been tasked with creating a monthly report for senior management detailing the security posture of the company. Which of the following is the MOST important element to include to ensure the report effectively communicates the company's current security status?

- (A) Detailed technical logs of all security incidents
- (B) **Graphical representation of incidents by category**
- (C) A complete list of all users and their access levels
- (D) Copies of recent phishing emails for demonstration

Explanation 390. Correct Answer: B. Graphical representation of incidents by category. A graphical

representation by category allows senior management to quickly understand the types and frequency of security incidents, which can help in decision-making and resource allocation.

Option A is incorrect. While technical logs are crucial for incident analysis, they may be too detailed and technical for a senior management report.

Option C is incorrect. While it's essential to manage user access levels, a complete list of all users and their access might be excessive for a monthly senior management report focused on the company's security posture.

Option D is incorrect. While examples of phishing emails can be educational, they are not crucial for a monthly report meant to provide an overview of the company's security status.

Question 391. A software developer in a company notices that a legitimate software tool they use is repeatedly flagged and quarantined by the company's security solution. Which of the following is the BEST action the cybersecurity team can take to address this without compromising security?

- (A) Turn off the antivirus solution
- (B) **Whitelist the software tool in the antivirus settings**
- (C) Decrease the security level of the antivirus
- (D) Install a different antivirus solution

Explanation 391. Correct Answer: B. Whitelist the software tool in the antivirus settings. Whitelisting allows the cybersecurity team to specify software or applications that are

considered safe and should not be flagged or quarantined by the antivirus solution.

Option A is incorrect. Turning off the antivirus solution would leave the system vulnerable to malware and other malicious threats.

Option C is incorrect. Decreasing the security level of the antivirus might reduce its effectiveness in detecting and blocking genuine threats.

Option D is incorrect. Simply installing a different antivirus solution does not guarantee that the tool won't be flagged again, and frequent switches can also be costly and time-consuming.

Question 392. Lucy, the IT security manager of a financial company, receives an automated alert that an employee attempted to email a document containing social security numbers to an external email address. Which of the following tools most likely generated this alert?

- (A) Network Intrusion Detection System (NIDS)
- (B) **Data Loss Prevention (DLP) solution**
- (C) Vulnerability Scanner
- (D) Packet Analyzer

Explanation 392. Correct Answer: B. Data Loss Prevention (DLP) solution. DLP solutions are specifically designed to monitor and control data transfers across an organization's network. In this case, the DLP detected sensitive data—social security numbers—being sent outside of the organization and alerted Lucy.

Option A is incorrect. NIDS detects and alerts on malicious activity on a network, but it doesn't typically scan for specific data types being transferred.

Option C is incorrect. Vulnerability scanners identify and report on vulnerabilities in a system but don't monitor data transfers.

Option D is incorrect. While packet analyzers can capture and analyze network traffic, they don't inherently generate alerts based on the specific content of data being transferred.

Question 393. A healthcare organization with patients worldwide is planning to set up a backup site for its medical data repository. They have been advised to consider geographic dispersion as part of their disaster recovery plan. Which of the following reasons is the LEAST valid for geographic dispersion in this scenario?

- (A) Mitigate risks of regional natural disasters
- (B) Offer redundancy in case of local power outages
- (C) Benefit from varying peak load times in different regions
- (D) **Ensure faster access speeds for global patients**

Explanation 393. Correct Answer: D. Ensure faster access speeds for global patients. Geographic dispersion's primary goal in a disaster recovery context is resilience and redundancy, not necessarily optimizing access speeds. While having servers in different locations can enhance speed for local users, in the context of a backup site for disaster recovery, the primary focus is on availability and redundancy, not speed.

Option A is incorrect. Geographic dispersion can help mitigate risks associated with regional natural disasters by ensuring that backup sites aren't impacted by the same disaster that affects the primary site.

Option B is incorrect. Regional power outages can be mitigated by having backup sites in different locations.

Option C is incorrect. Geographic dispersion can allow organizations to manage and distribute load more effectively by leveraging off-peak times in different regions.

Question 394. TechCo, a medium-sized enterprise, is planning to implement a solution to monitor, control, and restrict web access for its employees to improve productivity and enhance security. They also want to cache frequently accessed web content to reduce bandwidth consumption. Which solution would BEST fit TechCo's requirements?

- (A) Deploy a decentralized proxy on each departmental network
- (B) Set up a DNS-based filtering service
- (C) **Use a centralized proxy with caching capabilities**
- (D) Recommend browser extensions for web filtering to all employees

Explanation 394. Correct Answer: C. Use a centralized proxy with caching capabilities. A centralized proxy allows organizations to filter, monitor, and control web access from a central point. Additionally, proxies with caching capabilities can store frequently accessed web content, reducing the need for repeated downloads and thus saving bandwidth.

Option A is incorrect. A decentralized approach would make it challenging to consistently apply and enforce policies across the enterprise. It may also lead to inefficiencies in bandwidth usage as content caching would not be centralized.

Option B is incorrect. While a DNS-based filtering service can help in blocking access to certain malicious or inappropriate sites, it does not offer the centralized control or caching capabilities that a proxy does.

Option D is incorrect. Relying on browser extensions is a decentralized method that depends on user compliance and may not provide centralized control or caching capabilities.

Question 395. A software development company has just expanded its team and wants to ensure that in the event of a disaster, they can resume operations within a day. However, they have a limited budget for disaster recovery. Which of the following disaster recovery site types would be the most suitable for the company's needs?

- (A) Hot site with hourly data replication
- (B) Cold site with monthly data backups
- (C) **Warm site with daily backups**
- (D) Offsite tape backups

Explanation 395. Correct Answer: C. Warm site with daily backups. For the software development company's need to resume operations within a day, a warm site with daily backups would be ideal. The warm site has equipment and some level of data ready, which would facilitate a faster recovery compared to a cold site or just offsite backups.

Option A is incorrect. A hot site with hourly data replication might provide the quickest recovery, but it's also the most expensive option which may not align with the company's budget constraints.

Option B is incorrect. A cold site with monthly data backups would be cost-effective but might not allow for operations to resume within a day due to the time needed to set up equipment and restore the latest data.

Option D is incorrect. Offsite tape backups alone would not provide the infrastructure or equipment needed for quick recovery. It would also take considerable time to restore operations just from tape backups.

Question 396. A company has recently noticed an increased number of employees accessing social media sites during work hours, leading to decreased productivity. To counter this, the security administrator decides to limit access to these websites during peak working hours. Which firewall rule modification should the administrator make?

- (A) Implement an Intrusion Prevention System (IPS) rule to block social media content
- (B) Change the firewall rule to deny access to known social media IP addresses between 9 AM and 5 PM**
- (C) Use the firewall's URL filtering capability to blacklist social media URLs
- (D) Increase the firewall's bandwidth to accommodate the excess traffic

Explanation 396. Correct Answer: B. Change the firewall rule to deny access to known social media IP addresses between 9 AM and 5 PM.

Implementing a time-based rule that denies access to specific IP addresses (or ranges) associated with social media can be an effective way to restrict access during specified hours.

Option A is incorrect. An IPS is designed to detect and prevent malicious activities based on signatures. Blocking social media content is not typically its primary function.

Option C is incorrect. URL filtering would block access to the URLs entirely. The requirement is to block them only during specific hours.

Option D is incorrect. Increasing the firewall's bandwidth doesn't address the problem of employees accessing social media during work hours.

Question 397. As part of the annual security training, the IT department of XYZ Corp decides to launch a simulated phishing campaign. The aim is to assess employees' ability to identify and report phishing emails. Which of the following would be the MOST effective first step in ensuring the success of this campaign?

(A) Informing all employees about the campaign a week prior

(B) **Creating a realistic phishing email that closely resembles common threats**

(C) Offering rewards to employees who click on the

simulated phishing links

(D) Reviewing the results of the previous year's campaign

Explanation 397. Correct Answer: B. Creating a realistic phishing email that closely resembles common threats. For the phishing campaign to effectively assess employees' ability to recognize phishing threats, the simulated phishing email must be as realistic as possible. By making it closely resemble common threats, the IT department can gain a more accurate measure of the employees' awareness and response.

Option A is incorrect. Informing all employees about the campaign beforehand would defeat the purpose of the test, as they would be expecting a phishing email and thus be more likely to recognize and report it.

Option C is incorrect. Offering rewards to employees who click on the simulated phishing links would encourage risky behavior and is counterproductive to the goal of increasing security awareness.

Option D is incorrect. While reviewing results from previous campaigns can provide insights, it would not be the most effective first step in ensuring the success of the current campaign.

Question 398. An organization is planning to deploy a new web application that will be accessible from both the internal network and the internet. The application will communicate exclusively over HTTPS. The security administrator is asked to configure the firewall to allow the necessary traffic. Which of

the following should the administrator configure?

- (A) Allow port 21 and block all others
- (B) Allow port 443 and block all others**
- (C) Allow port 80 and block all others
- (D) Allow port 23 and block all others

Explanation 398. Correct Answer: B. Allow port 443 and block all others. HTTPS primarily uses port 443 for secure communication. Thus, allowing port 443 and blocking all others would ensure the secure operation of the web application.

Option A is incorrect. Port 21 is used for FTP (File Transfer Protocol), which is not relevant to HTTPS communication.

Option C is incorrect. While port 80 is used for HTTP, it does not provide the encryption that HTTPS does on port 443.

Option D is incorrect. Port 23 is used for Telnet, which is unrelated to secure web communication.

Question 399. The IT department of XYZ Corp is keen on preventing users from changing specific system settings, such as altering the firewall configurations. The majority of their infrastructure is based on Windows operating systems. Which of the following would be the most effective way to achieve this?

- (A) Use SELinux to enforce strict access controls
- (B) Utilize Group Policy to set and enforce policies related to system settings**
- (C) Deploy a third-party software solution to lock system settings

(D) Implement a user training program to guide users on system settings best practices

Explanation 399. Correct Answer: B. Utilize Group Policy to set and enforce policies related to system settings. Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. This can be used to enforce specific policies related to system settings in a Windows environment.

Option A is incorrect. SELinux (Security-Enhanced Linux) is primarily used in Linux environments to enforce mandatory access controls. It wouldn't be appropriate for a primarily Windows-based infrastructure.

Option C is incorrect. While third-party solutions may exist, leveraging built-in features like Group Policy is often more streamlined, cost-effective, and efficient.

Option D is incorrect. While user training is essential, relying solely on training without implementing technical controls is not effective in preventing users from altering system settings.

Question 400. During a routine check, an IT technician notices several files on a company server have been renamed with a ".locked" extension and there's a new file named "README_TO_RECOVER_FILES.txt" present in the root directory. Based on these indicators, which type of malicious activity is most likely in progress?

(A) Worm propagation

(B) Trojan horse execution

- (C) **Ransomware attack**
- (D) Logic bomb activation

Explanation 400. Correct Answer: C. Ransomware attack.

Ransomware is a type of malicious software that encrypts a victim's files, rendering them inaccessible. The attacker then demands a ransom from the victim in return for the decryption key. The renaming of files with a specific extension (like ".locked") and the presence of a ransom note (like "README_TO_RECOVER_FILES.txt") are typical indicators of a ransomware attack.

Option A is incorrect. Worm propagation refers to the spread of a standalone malware computer program that replicates itself to spread to other computers. It doesn't typically rename files or leave readable messages.

Option B is incorrect. A Trojan horse is malicious software that deceives users about its true intent. While it can deliver a ransomware payload, the described indicators more directly suggest ransomware activity.

Option D is incorrect. A logic bomb is a piece of code that executes a malicious function when certain conditions are met, but it doesn't necessarily leave the described file traces.

EXAM SIMULATOR #5

Questions 401-500

Question 401. The IT department at TechCorp Ltd has been instructed to ensure that critical system files remain unchanged to avoid potential security breaches. They want to implement a system that can provide alerts whenever there is an unauthorized change to these files. Which of the following would best serve this purpose?

- (A) Data Loss Prevention (DLP)
- (B) Intrusion Detection System (IDS)
- (C) File Integrity Monitoring (FIM)
- (D) Remote Monitoring and Management (RMM)

Question 402. Cybertech Corp. is reviewing its backup protocols to enhance security. They decided that before transferring backups to an offsite location, the data should be rendered unreadable to unauthorized individuals. Which backup strategy will ensure this requirement is met?

- (A) Use deduplication before storing backups
- (B) Store backups in proprietary formats
- (C) Encrypt backups before transfer
- (D) Compress backups using standard tools

Question 403. XYZ Corp is designing their new web application infrastructure. They want to ensure that all web traffic to and from their application is encrypted. In addition to selecting HTTPS as the protocol, which default port should they configure for this encrypted traffic?

- (A) 21
- (B) 80

- (C) 443
- (D) 25

Question 404. A company is developing a new web application that will be processing highly sensitive user data. They want to ensure that if the web server is compromised, attackers cannot directly access the database or other critical infrastructure.

Which of the following is the BEST strategy to achieve this objective?

- (A) Use strong authentication methods for the web application
- (B) Encrypt the user data at rest and in transit
- (C) Place the web server and the database server in separate network segments
- (D) Implement real-time monitoring of the web server

Question 405. After a major outage, CloudTech Services is reviewing their disaster recovery strategy. The company found out that after restoring from backup, several applications did not function properly due to configuration discrepancies. What would be the best approach to ensure a successful recovery in the future?

- (A) Prioritize applications for backup based on their importance
- (B) Implement differential backups in addition to full backups
- (C) Regularly conduct a full system recovery in a test environment
- (D) Use a third-party backup solution instead of an in-house solution

Question 406. GlobalBank has implemented a backup strategy where only the changes made since the last full backup are recorded. Considering the need to optimize storage and reduce backup times, the IT team performs this type of backup every day. What backup frequency and type is GlobalBank utilizing?

- (A) Incremental Backup daily
- (B) Differential Backup weekly
- (C) Full Backup bi-weekly
- (D) Snapshot Backup daily

Question 407. A company has recently deployed a new e-commerce application. The security team wants to ensure they can detect any unauthorized or malicious activities on the application. Which of the following would be the MOST effective way to achieve this goal?

- (A) Conduct a penetration test on the application
- (B) Install a firewall in front of the application
- (C) Implement continuous monitoring of the application's logs and activities
- (D) Provide training to users about secure browsing habits

Question 408. Sophia, a network administrator, is reviewing the logs from the company's Intrusion Detection System (IDS). She notices an increased amount of outbound traffic to an unfamiliar IP address. Upon deeper analysis, she found that the traffic consists of sensitive data being transferred. What type of malicious code might be responsible for this?

- (A) Ransomware
- (B) Adware
- (C) Data Exfiltration Malware
- (D) Keylogger

Question 409. ExamsDigest Enterprises wants to streamline their permission assignments. They decide that rather than assigning permissions to each user individually, they will group users based on departmental roles and then assign permissions to these groups. For example, all members of the “Marketing” role would have access to the marketing database. Which access control method is ExamsDigest Enterprises employing?

- (A) Rule-based access control
- (B) Mandatory Access Control (MAC)
- (C) Discretionary Access Control (DAC)
- (D) Role-Based Access Control (RBAC)

Question 410. A security administrator is considering a cryptographic solution for protecting data in transit between two servers located in the same data center. The primary goal is to ensure speed and efficiency in encryption and decryption processes. Which type of encryption would best meet this requirement?

- (A) Asymmetric encryption using RSA
- (B) Symmetric encryption using AES
- (C) Hybrid encryption using a combination of RSA and AES
- (D) Asymmetric encryption using ECC

Question 411. A large e-commerce company is deploying a new online payment system. The Chief Information Security Officer (CISO) is concerned about the security of cryptographic keys and wants to ensure they are protected from potential theft or compromise. Which tool should the CISO implement to provide the HIGHEST level of security for these keys?

- (A) Password vault

- (B) Software-based key storage
- (C) Hardware Security Module (HSM)
- (D) Cloud-based encryption service

Question 412. During a security audit, a company realized that a malicious actor was able to situate themselves on the network path, capturing TLS handshake messages between clients and the server. The attacker's goal is to weaken the encryption by influencing the cipher suite negotiation process. What type of network attack does this scenario depict?

- (A) ARP Poisoning
- (B) Downgrade Attack
- (C) SYN Flood
- (D) Ping of Death

Question 413. A software developer wants to store user passwords in a way that even if the database is compromised, attackers would not be able to retrieve the original passwords. What technique should the developer use to achieve this?

- (A) Symmetric encryption
- (B) Digital signing
- (C) Hashing
- (D) Steganography

Question 414. A company's IT department notices a sharp increase in account lockouts over the past two days, especially during non-business hours. While some accounts are from various departments, a majority are from the finance team. Which of the following is the MOST plausible explanation for these lockouts?

- (A) Scheduled maintenance by the IT department

- (B) Employees are sharing passwords within the finance team
- (C) An attacker is trying to gain unauthorized access
- (D) A recent password policy change requiring more frequent changes

Question 415. Carlos is responsible for managing IT services for a university. The university has numerous departments, each with its subdomain, like arts.university.com, science.university.com, and sports.university.com. Carlos wants a solution that ensures HTTPS security while being cost-effective. However, he's wary of potential risks. What might be a drawback of using a Wildcard Certificate for the university's subdomains?

- (A) It can secure only one subdomain
- (B) If compromised, all subdomains are at risk
- (C) It only validates the domain ownership, not the organization's identity
- (D) It's the most expensive certificate available

Question 416. SecureData Inc., a financial firm, recently experienced a system crash and needed to restore their database. While they had a full backup from the previous week, they realized that several days of transactions were missing. To prevent such data loss in the future, which backup strategy involving recording transactions can SecureData implement?

- (A) Implement differential backups
- (B) Use snapshot backups every hour
- (C) Enable database journaling
- (D) Configure RAID 5 for their storage

Question 417. A company has set up its firewall to allow web traffic through port 80 and port 443, while denying all other traffic by default. This setup is an example of which type of access control?

- (A) Role-Based Access Control (RBAC)
- (B) Mandatory Access Control (MAC)
- (C) Discretionary Access Control (DAC)
- (D) Rule-Based Access Control (RAC)

Question 418. During a routine security assessment, Jake, a penetration tester, discovers that by modifying a configuration file located in a public directory, he can assign himself administrative privileges in the application. What type of vulnerability is Jake exploiting?

- (A) Cross-Site Scripting (XSS)
- (B) Privilege Escalation
- (C) SQL Injection
- (D) Insecure Direct Object Reference (IDOR)

Question 419. A school wants to prevent its students from accessing inappropriate websites during class hours. The IT department decides to implement a solution that blocks requests to specific domain names associated with inappropriate content. Which of the following security solutions would best address this need?

- (A) Firewall filtering based on IP addresses
- (B) Intrusion Detection System monitoring
- (C) Virtual Private Network (VPN) enforcement
- (D) DNS filtering with a blacklist

Question 420. A financial firm has just experienced a cyber attack, and the IT team identified a piece of malware that evaded their traditional antivirus solutions. The CISO now wants to not only detect but also be able to analyze and respond to such advanced threats in real-time. Which solution should the firm consider implementing?

- (A) Vulnerability Scanner
- (B) Intrusion Prevention System (IPS)
- (C) Endpoint Detection and Response (EDR)
- (D) Patch Management System

Question 421. During a routine audit of the corporate servers, the system administrator discovers that a week's worth of security logs are missing from one of the key application servers. Which of the following is the MOST likely reason for this occurrence?

- (A) The logging service experienced a malfunction
- (B) There was insufficient storage space for the logs
- (C) A malware attack aimed to erase traces of intrusion
- (D) The time zone setting was incorrectly configured

Question 422. A financial company is designing a new system that needs to ensure data is accessed based on classifications and clearance levels of the users. Which of the following access control models BEST fits this requirement?

- (A) Role-Based Access Control (RBAC)
- (B) Discretionary Access Control (DAC)
- (C) Mandatory Access Control (MAC)
- (D) Attribute-Based Access Control (ABAC)

Question 423. TechSolutions Inc., a rapidly growing startup, is expanding its workforce to meet its customer demands. As part of this expansion, they need to ensure their IT infrastructure can accommodate the influx of new employees without compromising performance or security. Which of the following should be TechSolutions' primary focus during this expansion phase?

- (A) Adopting a Zero Trust Network Architecture
- (B) Increasing the frequency of vulnerability assessments
- (C) Implementing capacity planning
- (D) Deploying additional firewalls and intrusion detection systems

Question 424. Emily, a cybersecurity analyst, has been tasked with gathering preliminary information about a target organization without directly interacting with its systems. She decides to collect data from third-party sources, search engines, public records, and other online platforms without sending any packets to the target. Which phase of penetration testing is Emily currently engaged in?

- (A) Active reconnaissance
- (B) Passive reconnaissance
- (C) Vulnerability scanning
- (D) Threat hunting

Question 425. During the setup of a secure communication channel, Alice and Bob need to agree upon a shared secret key without sending the key directly to each other, as they fear eavesdropping. Which protocol would best facilitate this requirement?

- (A) RSA

- (B) HMAC
- (C) Diffie-Hellman
- (D) AES

Question 426. A company plans to upgrade its email server to ensure that email transmission between their mail server and client applications is encrypted. Which of the following protocols would be the most appropriate for this purpose?

- (A) HTTP
- (B) FTP
- (C) IMAP over SSL/TLS
- (D) SNMP

Question 427. A medium-sized company has just deployed a new file server for the HR department. They want to ensure that only HR employees can view and edit HR-specific documents, while the IT department should only be able to perform system maintenance tasks. What should the company implement to achieve this requirement?

- (A) Install a firewall between the HR and IT departments
- (B) Implement an Access Control List (ACL) for the file server
- (C) Enforce a strong password policy for the HR department
- (D) Enable full disk encryption on the file server

Question 428. Carla, a security analyst, receives an alert that one of the company's server certificates may have been exposed in a recent data breach. What is the most immediate action Carla should take to ensure that the exposed certificate cannot be used maliciously?

- (A) Request a new certificate from the CA

- (B) Update the company firewall rules
- (C) Add the certificate to the Certificate revocation list (CRL)
- (D) Perform a vulnerability assessment on the server

Question 429. DataFin, a financial analytics firm, experienced a minor fire incident in one of its server rooms. Fortunately, they had backups stored in another wing of the building, allowing for quick data recovery. However, management realizes that in a major disaster, both primary and backup data might be destroyed. To address this, which backup strategy should DataFin consider?

- (A) Mirror Backup
- (B) Local Storage Backup
- (C) Incremental Backup
- (D) Offsite Backup

Question 430. An online retailer is considering various methods to protect its customers' credit card information. Instead of storing the actual credit card numbers in their database, they opt for a solution that replaces the numbers with unrelated, random values. What is this method called?

- (A) Symmetric encryption
- (B) Digital watermarking
- (C) Hashing
- (D) Tokenization

Question 431. The IT team at TechnoCorp has noticed a consistent pattern over the last week where a particular server's CPU usage spikes to 100% between 2:00 AM and 4:00 AM, a time when there's typically minimal user activity. What could

be the MOST probable reason for this?

- (A) The server is automatically updating its software
- (B) An employee is running a heavy computational task
- (C) The server is undergoing a DDoS attack
- (D) Malware is performing cryptomining activities

Question 432. A journalist wants to send a confidential message to her editor without raising suspicion. Instead of sending a coded or encrypted text, she embeds the message within a harmless-looking photograph. What method is she employing to keep the message concealed?

- (A) Digital signature
- (B) Tunneling
- (C) Steganography
- (D) Chaining

Question 433. Ella, a security analyst, is reviewing the logs of a web application and notices that an attacker attempted to use the following input in a login form: ' OR '1'='1' --. This input was used in an effort to manipulate the application's backend database. What type of injection attack is this an example of?

- (A) XML Injection
- (B) Command Injection
- (C) SQL Injection
- (D) LDAP Injection

Question 434. During a security audit, it was found that an application was using plain hashes for storing passwords. The security team recommended a method that involves using the original password along with a salt and then rehashing it multiple times. What is this method known as?

- (A) Key clustering
- (B) Rainbow table prevention
- (C) Key rotation
- (D) Key stretching

Question 435. A university's IT department provides access to its student records for training purposes to new hires. To protect student identities, they replace the real names and social security numbers with fictitious ones while maintaining the database's original format. Which technique is the IT department utilizing?

- (A) Digital signing
- (B) Data masking
- (C) Steganography
- (D) Data deduplication

Question 436. StreamNet, a popular online streaming service, is planning to launch in three new countries. They anticipate a substantial increase in users and concurrent streams. To ensure that the service remains uninterrupted and provides a seamless experience to new users, which action related to capacity planning should StreamNet prioritize?

- (A) Investing in content encryption and DRM
- (B) Increasing marketing and promotional activities in the new countries
- (C) Implementing stronger user authentication methods
- (D) Expanding and optimizing their infrastructure to handle the projected growth

Question 437. The IT department of an e-commerce company is configuring access controls for a new online product

inventory system. They want the sales team to update the inventory levels and product details but don't want them to access financial data stored in the same system. Which access control principle is the IT department applying?

- (A) Least Privilege
- (B) Role-Based Access Control (RBAC)
- (C) Mandatory Access Control (MAC)
- (D) User-Based Access Control (UBAC)

Question 438. The IT department of XYZ Corp noticed that server logs are recording user login attempts during non-business hours, specifically between 2:00 AM and 3:00 AM, a time when no scheduled tasks or backups are set to run. Which of the following is the MOST plausible explanation for this unusual activity?

- (A) The company's employees are working overtime
- (B) There might be a time zone misconfiguration on the server
- (C) An unauthorized user is trying to gain access to the server
- (D) The server is automatically installing security patches

Question 439. A financial institution processes thousands of credit card transactions daily. To ensure the security and integrity of these transactions, the security officer wants to employ a solution that will safely manage and store cryptographic keys. Which of the following would be the MOST suitable solution?

- (A) Trusted Platform Module (TPM)
- (B) Full Disk Encryption (FDE)

- (C) Hardware Security Module (HSM)
- (D) Software Key Repository

Question 440. XYZ Corp recently faced a ransomware attack that encrypted critical data files. The company's IT team was unable to decrypt the files but had a recent backup available. However, when they tried to restore the data, they found out the backup was corrupted. Which of the following best practices would have helped XYZ Corp in ensuring the integrity of their backups?

- (A) Regularly testing backup restoration processes
- (B) Storing backups in the same directory as original files
- (C) Increasing the frequency of backups to every hour
- (D) Encrypting backups with a strong encryption algorithm

Question 441. An e-commerce company stores millions of customer transaction records in their primary database. They have decided to enhance their security posture by applying encryption to protect sensitive data. However, they don't want to encrypt the entire server storage, just the data within the database. Which encryption approach should the company adopt to meet their objective?

- (A) Full-disk Encryption
- (B) File-level Encryption
- (C) Volume-level Encryption
- (D) Database-level Encryption

Question 442. A database administrator is concerned about identical hashes being produced for users who select the same password. To mitigate this risk, what cryptographic technique should the administrator implement?

- (A) Digital signature
- (B) Salting
- (C) Key stretching
- (D) Symmetric encryption

Question 443. After a recent data breach, a multinational corporation is evaluating its cryptographic practices. The Chief Security Officer (CSO) determines that the manual management of cryptographic keys has become too complex due to the scale of the operations. Which tool would BEST address the CSO's concern while ensuring robust security practices?

- (A) Password Management System
- (B) Secure File Transfer Protocol (SFTP)
- (C) Trusted Platform Module (TPM)
- (D) Key Management System (KMS)

Question 444. After a security incident, a forensic investigation revealed that a compromised internal workstation was communicating with a known malicious IP address. To prevent further communication, the security team decided to take immediate action. Which of the following is the BEST immediate action to ensure the workstation cannot communicate with that IP?

- (A) Implement a block rule on the web filter for the IP address
- (B) Disable the network port of the compromised workstation
- (C) Use a honeypot to divert the traffic from the malicious
- (D) Update the firewall's firmware

Question 445. Jennifer, an IT administrator, is asked to onboard a new remote employee for a sales role. Which of the following is the BEST approach for provisioning the user account?

- (A) Assign the new user the same access privileges as the CEO because they might require all resources
- (B) Provide the new user with administrative rights to ensure they can install and configure any needed software
- (C) Use the access privileges from a template of a salesperson to provide the required resources
- (D) Allow the new user to decide and self-select the necessary access based on their job role

Question 446. The IT department of a large organization receives reports from employees that they are unable to access certain resources on the network. Upon investigation, the IT department discovers that the Access Control List (ACL) settings have been recently modified. Which of the following would be the PRIMARY reason to review and modify the ACL settings?

- (A) To balance the network load
- (B) To update the organization's firewall rules.
- (C) To ensure appropriate access rights to resources
- (D) To update the organization's password policy

Question 447. TechWorld Corp is concerned about cybercriminals sending emails that appear to come from its domain to deceive its clients. The company wants to implement a solution that would allow receiving email servers to validate that an email claiming to come from TechWorld Corp's domain indeed originates from an approved server. Which of the following should the company implement?

- (A) SMTP authentication
- (B) DKIM
- (C) POP3 over SSL
- (D) S/MIME

Question 448. A cloud-based collaboration tool used by a company displays a warning to a user stating, “You are logged in from two locations.” However, the user has only one active session on their workstation. What should be the primary concern for the security team?

- (A) The user might be using multiple devices
- (B) There's a potential misconfiguration in the tool's settings
- (C) The collaboration tool is facing an outage
- (D) There might be unauthorized access to the user's account

Question 449. A company is looking for a cryptographic solution that provides an immutable and transparent record of all transactions in a distributed ledger system. Which of the following would BEST meet this requirement?

- (A) Symmetric key algorithm
- (B) Public key infrastructure
- (C) Blockchain
- (D) Digital watermark

Question 450. TechCorp is collaborating with SoftTech, a business partner. To streamline collaboration without managing multiple accounts, TechCorp wants its employees to use their existing credentials to access SoftTech’s online project management system. Which of the following approaches would BEST enable this functionality?

- (A) TechCorp should create new accounts for its employees on SoftTech's system
- (B) SoftTech should allow anonymous access for TechCorp's employees
- (C) TechCorp should implement federation between its identity provider and SoftTech's service provider
- (D) SoftTech should reset all passwords and provide them to TechCorp's employees

Question 451. GlobalTech is implementing a disaster recovery plan and wants to ensure continuous availability with no data loss. They have decided to use replication as a backup strategy. Which of the following replication techniques should GlobalTech implement to achieve their objective?

- (A) Periodic replication scheduled daily
- (B) Asynchronous replication with hourly synchronization
- (C) Synchronous replication
- (D) Snapshot replication every 30 minutes

Question 452. An e-commerce website suddenly experiences a sharp increase in traffic, causing the website to become slow and occasionally inaccessible. The IT team observes that a large number of requests are originating from multiple IP addresses spread across various countries. What type of network attack is the e-commerce website likely experiencing?

- (A) Man-in-the-middle attack
- (B) DNS spoofing
- (C) Distributed denial-of-service (DDoS) attack
- (D) ARP poisoning

Question 453. A software development company is working on a mobile banking application. They want to ensure that sensitive operations like cryptographic processes and biometric data validation are isolated from the main operating system to prevent potential tampering. Which tool should they consider implementing to achieve this objective?

- (A) Hardware Security Module (HSM)
- (B) Key Management System (KMS)
- (C) Secure enclave
- (D) Trusted Platform Module (TPM)

Question 454. A popular social media platform allows third-party applications to access user data and post on behalf of users. To avoid sharing user passwords with third-party applications and provide limited, scoped access, which authentication method should the platform use?

- (A) Embed user passwords in the application's code
- (B) Use basic authentication with username and password for every request
- (C) Implement Single Sign-On (SSO) using OAuth to provide token-based access
- (D) Rely solely on CAPTCHA for third-party app authentication

Question 455. A company has noticed an increase in malware infections over the past month. After investigating, it was determined that the infections were caused by employees visiting websites that were newly registered but had malicious intent. Which of the following would be the BEST approach to mitigate this threat?

- (A) Implement a block rule to deny access to all websites

- (B) Use a web filter that incorporates domain reputation checks and blocks domains registered recently
- (C) Set the web filter to block all websites not categorized as "Business"
- (D) Enforce multi-factor authentication for all internet-based applications

Question 456. MetroTech recently experienced an incident where an employee mistakenly deleted a portion of their database. The IT team was able to restore the data using a backup snapshot taken 24 hours prior. However, some data loss still occurred. Which of the following recommendations would minimize data loss in a similar situation in the future?

- (A) Configure backup snapshots to be taken on a weekly basis
- (B) Employ a differential backup solution in addition to snapshots
- (C) Increase the storage capacity for backups
- (D) Use an hourly snapshot backup schedule

Question 457. Alice receives an email from Bob with an attached document. She wants to verify both the authenticity of the sender and the integrity of the attached document. Which of the following should Bob have used before sending the email?

- (A) Encrypt the document with his private key
- (B) Hash the document
- (C) Encrypt the document with Alice's public key
- (D) Sign the document with his private key

Question 458. An international company, GlobalTech, is using several web applications hosted by different vendors. To ensure

their employees can access these applications without having to remember multiple sets of credentials, they want to implement a solution that can securely exchange user authentication information between the company and the service providers.

What should GlobalTech implement?

- (A) Integrate each application with an independent LDAP server
- (B) Implement SSO using Security Assertions Markup Language (SAML)
- (C) Embed encrypted user credentials within the URL of each application
- (D) Rely on public API keys shared between the company and each vendor

Question 459. A user wants to send a confidential email to their colleague and ensure that only the intended recipient can read it. The user also wants to provide assurance to the recipient that the email was indeed sent by them. Which encryption method should the user employ to accomplish this?

- (A) Use symmetric encryption with a shared key
- (B) Use asymmetric encryption and encrypt the email with the recipient's public key
- (C) Use asymmetric encryption, encrypt the email with the user's private key
- (D) Use asymmetric encryption, first sign the email with the user's private key, then encrypt it with the recipient's public key

Question 460. DigitalFront, an e-commerce company, is expecting a surge in traffic during their upcoming annual sale event. They want to ensure that their website and applications can handle the anticipated increase in user activity without any

performance degradation. Which of the following steps is MOST relevant to achieving this goal?

- (A) Increasing the frequency of security audits
- (B) Implementing capacity planning specifically focused on technology
- (C) Adopting multi-factor authentication for all users
- (D) Investing in advanced threat intelligence solutions

Question 461. Sarah, a security analyst, is concerned about potential man-in-the-middle attacks on the company's internal portal. To mitigate this risk, she recommends obtaining a digital certificate from a trusted entity. Which of the following is responsible for issuing such certificates?

- (A) Key distribution center
- (B) Certificate authority (CA)
- (C) Tokenization system
- (D) Security incident event manager

Question 462. A security analyst discovers that an external IP address has been repeatedly trying every possible combination of characters to gain access to the company's VPN portal for the past two days. Which type of password attack is this MOST likely describing?

- (A) Password Spraying
- (B) Dictionary Attack
- (C) Rainbow Table Attack
- (D) Brute Force Attack

Question 463. A graphic design company frequently works with large files such as videos and high-resolution images. These files are stored on a dedicated storage volume in their server.

While they need to secure this data, they don't want to encrypt individual files due to the volume of data and frequent access needs. Which encryption approach is most appropriate for this scenario?

- (A) File-level Encryption
- (B) Full-disk Encryption
- (C) Transport-layer Encryption
- (D) Volume-level Encryption

Question 464. Sarah is a project manager and is working on a document that she owns. She wants to grant specific permissions to certain team members, allowing some to edit and others only to view the document. Which of the following access control models would BEST allow Sarah to accomplish this?

- (A) Mandatory Access Control (MAC)
- (B) Role-Based Access Control (RBAC)
- (C) Discretionary Access Control (DAC)
- (D) Attribute-Based Access Control (ABAC)

Question 465. MegaCorp is transitioning to a cloud-based infrastructure and wants to allow its employees to access multiple cloud services without re-entering their credentials every time. They currently have an on-premises LDAP directory in place. Which approach should MegaCorp take to provide a seamless authentication experience?

- (A) MegaCorp should abandon their LDAP directory and create individual accounts for each cloud service
- (B) Integrate their LDAP with a Single Sign-On (SSO) solution that supports cloud services
- (C) Store passwords in a plaintext file for users to access

and login to cloud services manually

(D) Force users to change passwords every day to enhance security across all cloud platforms

Question 466. A global manufacturing company wants to ensure its employees worldwide do not access websites promoting hate speech, gambling, or explicit content during working hours. To meet this requirement, which web filtering technique would be the most efficient?

(A) Deploy a centralized proxy with location-based filtering

(B) Use a blacklist of specific URLs known to contain such content

(C) Implement content categorization and block undesired categories

(D) Monitor internet usage logs and reprimand violators

Question 467. During an IT audit, a company's encryption practices come under scrutiny. The IT auditor recommends increasing the encryption key length for certain applications to improve security. What is the PRIMARY reason to increase the encryption key length?

(A) To speed up encryption and decryption processes

(B) To ensure compatibility with older systems

(C) To reduce the possibility of a brute force attack

(D) To reduce the key management overhead

Question 468. PharmaCorp, a pharmaceutical company, wants to ensure that its researchers cannot transfer proprietary formulas and research data to external storage devices or cloud storage. The company needs a solution to prevent such transfers while allowing other types of data to be transferred. What

should they implement?

- (A) Web Application Firewall (WAF)
- (B) Data Encryption Tool
- (C) Data Loss Prevention (DLP)
- (D) Virtual Private Network (VPN)

Question 469. An online banking platform wants to improve its customer verification process when users open a new account. Which of the following identity proofing methods would be the MOST secure for this purpose?

- (A) Asking users to select a security question and answer from a list
- (B) Requiring users to upload a photo of a government-issued ID and a selfie
- (C) Sending a verification code to the user's email address
- (D) Prompting users to provide their favorite color

Question 470. Sarah is working on a project where she needs to validate the integrity and authenticity of assets over time, without a centralized authority. Which technology would be most appropriate for this use case?

- (A) Digital signature
- (B) Key escrow
- (C) Blockchain
- (D) Key management system

Question 471. After a recent cyber attack on a corporation's central database, the IT department has been tasked with enhancing the security of their network infrastructure. Which of the following would be the BEST technique to ensure that different departments, like HR and Finance, cannot access each

other's sensitive data?

- (A) Implement network segmentation based on departments
- (B) Upgrade the bandwidth of the entire network
- (C) Use a single strong password for all departments
- (D) Move all department data to the cloud

Question 472. A finance department employee, Maya, is transferred to the HR department. The IT department is considering her access requirements. Which of the following actions aligns best with the principle of least privilege?

- (A) Retain Maya's access to the finance system and grant additional access to the HR system
- (B) Remove all previous access rights and provide her access solely to the HR system
- (C) Grant Maya administrative rights to ease her transition between departments
- (D) Limit Maya's access to read-only for both finance and HR systems for a transitional period

Question 473. A financial institution, BankCorp, has recently experienced a surge in phishing attacks targeting its employees. These attacks often involve URLs that look similar to legitimate ones but have slight variations. To reduce the risk of employees accidentally accessing these malicious sites, which measure should BankCorp implement?

- (A) Implement a Domain Name System (DNS) firewall
- (B) Employ URL scanning to identify and block malicious URLs
- (C) Rely on manual reporting of suspicious URLs by employees

(D) Use a Virtual Private Network (VPN) to redirect all employee web traffic

Question 474. The IT team at a manufacturing company is deploying an IoT-based monitoring system for their machinery. They want to ensure that these IoT devices, if compromised, cannot adversely affect their main corporate network. What should they implement to achieve this?

- (A)** Install antivirus software on all IoT devices
- (B)** Regularly patch and update the IoT device firmware
- (C)** Place the IoT devices on a dedicated VLAN
- (D)** Enable multi-factor authentication for IoT devices

Question 475. The content filtering logs at a retail company display multiple instances of blocked access to a file download URL ending with “.exe”. The source IP address belongs to a point of sale (POS) terminal. What should be the primary concern for the security team?

- (A)** The POS terminal might have outdated software
- (B)** There's a possible misconfiguration in the content filtering rules
- (C)** The POS terminal might be compromised and trying to download malicious executables
- (D)** The company's internet speed is too slow

Question 476. A company wants to implement a solution that verifies the software integrity of remote servers before allowing them to connect to the primary network. Which of the following solutions BEST achieves this objective through attestation?

- (A)** Host-based firewall
- (B)** Whitelisting application

- (C) Remote attestation
- (D) VPN tunneling

Question 477. ABC Tech has a mixed environment with both Linux and Windows servers. They want to ensure that processes running on their Linux servers only have access to specific resources and are restricted from performing certain actions. Which of the following tools would be most appropriate for this task?

- (A) Use Group Policy on their Windows servers and apply it to Linux servers
- (B) Implement a strict user training regimen to inform users about security best practices
- (C) Enable Security-Enhanced Linux (SELinux) in enforcing mode
- (D) Limit user access to Linux servers

Question 478. Liam, a security analyst, is investigating a potential breach. He discovers that a malicious actor sent requests to the server by altering HTTP headers to impersonate another user, thereby gaining unauthorized access. Which type of application attack is this?

- (A) Cross-Site Request Forgery (CSRF)
- (B) Cross-Site Scripting (XSS)
- (C) HTTP Header Forgery
- (D) Session Hijacking

Question 479. ABC Corp has recently faced a security breach due to a contractor connecting an infected laptop to the corporate network. Management wants to implement a solution that would ensure that any device connecting to the corporate

network meets the company's security standards, including up-to-date antivirus definitions. Which solution should ABC Corp consider?

- (A) Intrusion Detection System (IDS)
- (B) Virtual Private Network (VPN)
- (C) Network Access Control (NAC)
- (D) Web Application Firewall (WAF)

Question 480. CyberFirm has been facing issues with phishing campaigns where attackers spoof their domain to send fraudulent emails. They already implemented DKIM to sign their emails but want an additional measure to specify which mail servers are authorized to send emails on behalf of their domain. Which security measure should CyberFirm adopt?

- (A) SPF
- (B) PGP
- (C) SSL certificate
- (D) IMAP

Question 481. A web application requires users to authenticate using a token sent to their email. Alex, a security analyst, observes that once logged in, if he presents the same token again, he is granted access without any restrictions. What type of vulnerability does this situation depict?

- (A) Cross-Site Request Forgery (CSRF)
- (B) Replay Attack
- (C) Man-in-the-Middle (MitM) Attack
- (D) Cross-Site Scripting (XSS)

Question 482. A large law firm has a centralized document repository where lawyers store client information, legal drafts,

and other sensitive data. A new paralegal, Jenna, joins the firm and needs to be able to view client documents but should not be able to modify or delete them. Which type of permission should be granted to Jenna?

- (A) Read-Only
- (B) Full Control
- (C) Modify
- (D) Execute

Question 483. The IT department of a software development company wants to ensure that only company-approved development tools can be executed in their development environment, preventing any unauthorized or potentially harmful software from running. What should the IT department employ to achieve this?

- (A) Implement network segmentation
- (B) Conduct regular vulnerability assessments
- (C) Install a stateful firewall
- (D) Establish an application allow list

Question 484. A company is implementing a system to ensure that code released to production is both unaltered and approved by a specific team member. Which of the following cryptographic techniques should they implement?

- (A) Symmetric encryption of the code
- (B) Hashing the code with SHA-256
- (C) Encrypting the code with the team member's public key
- (D) Digital signature by the team member

Question 485. During an organization's security review, the cybersecurity analyst noticed that there were multiple failed

login attempts for different user accounts, each with a few commonly used passwords. What type of password attack does this scenario BEST describe?

- (A) Brute Force Attack
- (B) Dictionary Attack
- (C) Credential Stuffing
- (D) Password Spraying

Question 486. A project manager is working on a new product launch and has documents with sensitive financial projections on her local computer. She occasionally shares these documents with select board members via email. While she wants to keep the financial documents secure, she doesn't want to encrypt all the data on her computer. Which encryption approach should she utilize?

- (A) Full-disk Encryption
- (B) Transport-layer Encryption
- (C) File-level Encryption
- (D) Partition Encryption

Question 487. A financial institution is looking to adopt an encryption algorithm for its transactions that is considered to be very secure due to its longer key length, compared to older standards. Which encryption algorithm best fits this description?

- (A) DES
- (B) Blowfish
- (C) RSA
- (D) AES-256

Question 488. The IT team of XYZ Corp received an alert that an employee's account was used to access the company's portal

from Paris at 2:00 PM and then from Tokyo at 2:30 PM. The employee is currently on a business trip to Paris. What could this alert be indicating?

- (A) The employee quickly traveled from Paris to Tokyo
- (B) The company's time zone settings are misconfigured
- (C) There's a possible VPN misconfiguration on the employee's computer
- (D) The employee's account might have been compromised

Question 489. Global Corp received a report that some of its customers received phishing emails that seemed to originate from the company's domain. The IT team checked and confirmed that SPF and DKIM configurations were correctly set. What additional email security measure can Global Corp implement to provide clear policies on how the emails should be treated if they don't align with SPF and DKIM?

- (A) Enabling TLS encryption
- (B) Implementing DMARC policies
- (C) Setting up a new SMTP server
- (D) Increasing email retention period

Question 490. A financial institution plans to provide access to its database for third-party developers to create new applications. However, they want to ensure that the developers do not see the actual data but instead work with a disguised version that retains the data's original structure. What technique is the financial institution considering?

- (A) Tokenization
- (B) Data masking
- (C) Encryption
- (D) Digital watermarking

Question 491. While reviewing web server logs, Sarah, a security analyst, notices a pattern of requests containing “..%2F..” in the URLs. She suspects this might be an attempt to exploit a vulnerability. Which type of application attack is likely being attempted?

- (A) Command Injection
- (B) Cross-Site Scripting (XSS)
- (C) Directory Traversal
- (D) Cross-Site Request Forgery (CSRF)

Question 492. A financial firm outsources its payment processing to a third-party service provider. After a series of fraudulent transactions, it was discovered that the service provider was not employing the latest encryption standards when transmitting data. Which vulnerability related to supply chain does this scenario highlight?

- (A) Inadequate vendor background checks
- (B) Service provider's outdated security practices
- (C) Deficient hardware components from a supplier
- (D) Software with embedded backdoors

Question 493. A security analyst is evaluating security enhancements for a series of laptops that will store highly confidential data. The analyst wants to ensure that stored data remains encrypted and the integrity of the boot process is maintained. Which of the following would BEST meet this requirement?

- (A) Installing antivirus software on each laptop
- (B) Enabling a software-based full-disk encryption
- (C) Implementing a BIOS password
- (D) Utilizing a Trusted Platform Module (TPM)

Question 494. An organization is choosing a hash function for digital signatures. They want to ensure that it is resistant to scenarios where an attacker might produce two different messages having the same hash. Which type of attack are they trying to defend against?

- (A) Side-channel Attack
- (B) Replay Attack
- (C) Birthday Attack
- (D) Ciphertext-only Attack

Question 495. At ExamsDigest, employees can access the company's cloud-based storage system. However, access to certain files within the storage is determined by the employee's department, job title, and years of service. For instance, senior managers in the finance department with more than five years of service can view the company's financial forecasts. Which access control model is ExamsDigest using?

- (A) Rule-Based Access Control (RAC)
- (B) Role-Based Access Control (RBAC)
- (C) Attribute-Based Access Control (ABAC)
- (D) Discretionary Access Control (DAC)

Question 496. After a recent system upgrade, CloudTech Corp. decided to validate the efficiency and reliability of its new data processing system. To do this, they run the new system alongside the old one and compare the outcomes. This way, they aim to ensure that the new system is both robust and capable of handling the current workload. What kind of testing is CloudTech Corp. utilizing?

- (A) Load Testing
- (B) Failover Testing

- (C) Parallel Processing Testing
- (D) Simulation Testing

Question 497. SecureNet Inc. recently upgraded their security infrastructure. To validate how the new system would respond in real-world scenarios without exposing it to actual risks, they decide to imitate certain cyber threats in a controlled environment. Which type of test is SecureNet Inc. planning to conduct?

- (A) Penetration Testing
- (B) Simulation Testing
- (C) Vulnerability Assessment
- (D) Failover Testing.

Question 498. A marketing team is collaborating on a new campaign and requires access to a shared folder. However, they shouldn't be able to modify files created by others. How should permissions be set on this shared folder?

- (A) Assign the marketing team full control
- (B) Allow the marketing team read-only access
- (C) Assign the marketing team write-only access
- (D) Assign the marketing team modify permission but deny the delete permission

Question 499. An organization's e-commerce platform experienced a data breach where attackers exploited a known vulnerability. Post-incident analysis revealed that a patch was available for this vulnerability two months before the breach but was not applied. Which of the following would have been the MOST effective measure to prevent this breach?

- (A) Implementing stronger user authentication methods

- (B) Increasing network monitoring for signs of malicious activity
- (C) Applying the available patch in a timely manner
- (D) Migrating to a different e-commerce platform

Question 500. A security analyst is reviewing network logs and notices that an attacker positioned in between the user and the target website is intercepting and potentially modifying the user's communications before passing them on to the intended destination. This malicious activity occurs transparently, with neither the user nor the target website being aware. What type of network attack is being described?

- (A) Replay Attack
- (B) Smurf Attack
- (C) On-path Attack
- (D) Spoofing Attack

Answers 401-500

Question 401. The IT department at TechCorp Ltd has been instructed to ensure that critical system files remain unchanged to avoid potential security breaches. They want to implement a system that can provide alerts whenever there is an unauthorized change to these files. Which of the following would best serve this purpose?

- (A) Data Loss Prevention (DLP)
- (B) Intrusion Detection System (IDS)

- (C) **File Integrity Monitoring (FIM)**
- (D) Remote Monitoring and Management (RMM)

Explanation 401. Correct Answer: C. File Integrity Monitoring (FIM). File Integrity Monitoring (FIM) tools monitor and detect changes in files that may indicate a breach, malware infection, or other unauthorized activity. By tracking and reporting on file change patterns, FIM helps ensure the integrity and confidentiality of data.

Option A is incorrect. Data Loss Prevention (DLP) focuses on preventing unauthorized data transfers or leaks from the organization, not on monitoring file changes.

Option B is incorrect. An Intrusion Detection System (IDS) primarily detects unauthorized access or attacks on a network. While it can identify some unauthorized file changes, it isn't specifically designed for file integrity monitoring.

Option D is incorrect. Remote Monitoring and Management (RMM) tools primarily allow IT professionals to monitor and manage endpoints, networks, and computers remotely. They don't specifically focus on file integrity.

Question 402. Cybertech Corp. is reviewing its backup protocols to enhance security. They decided that before transferring backups to an offsite location, the data should be rendered unreadable to unauthorized individuals. Which backup strategy will ensure this requirement is met?

- (A) Use deduplication before storing backups
- (B) Store backups in proprietary formats

- (C) **Encrypt backups before transfer**
- (D) Compress backups using standard tools

Explanation 402. Correct Answer: C. Encrypt backups before transfer. Encryption transforms data into a format that can only be read by someone who possesses the decryption key. By encrypting backups before transferring, Cybertech Corp. ensures that even if unauthorized individuals access the backup data, they won't be able to understand its contents.

Option A is incorrect. Deduplication reduces the storage space required for backups by eliminating redundant data but doesn't make data unreadable to unauthorized individuals.

Option B is incorrect. Using proprietary formats may obscure the data for some unauthorized users, but it does not provide the robust protection encryption does.

Option D is incorrect. Compressing backups using standard tools optimizes storage but does not ensure data confidentiality.

Question 403. XYZ Corp is designing their new web application infrastructure. They want to ensure that all web traffic to and from their application is encrypted. In addition to selecting HTTPS as the protocol, which default port should they configure for this encrypted traffic?

- (A) 21
- (B) 80
- (C) **443**
- (D) 25

Explanation 403. Correct Answer: C. 443. Port 443 is the default port used for HTTPS (HTTP over SSL/TLS) traffic. It ensures that web traffic is encrypted and provides a secure communication channel between the client and the server.

Option A is incorrect. Port 21 is the default port for FTP (File Transfer Protocol), which is used for transferring files, not encrypted web traffic.

Option B is incorrect. Port 80 is the default port for HTTP, which is unencrypted.

Option D is incorrect. Port 25 is the default port for SMTP (Simple Mail Transfer Protocol), which is used for email transmission, not encrypted web traffic.

Question 404. A company is developing a new web application that will be processing highly sensitive user data. They want to ensure that if the web server is compromised, attackers cannot directly access the database or other critical infrastructure. Which of the following is the BEST strategy to achieve this objective?

- (A) Use strong authentication methods for the web application
- (B) Encrypt the user data at rest and in transit
- (C) **Place the web server and the database server in separate network segments**
- (D) Implement real-time monitoring of the web server

Explanation 404. Correct Answer: C. Place the web server and the database server in separate network segments. By

placing the web server and the database server in separate network segments, the company can achieve isolation. This means that even if the web server is compromised, attackers would still have to breach additional security measures to access the database server or other critical parts of the infrastructure.

Option A is incorrect. While using strong authentication methods is important, it doesn't provide isolation between the web server and other critical components.

Option B is incorrect. Encrypting user data is essential for data protection, but it doesn't provide network-based isolation between the web server and other systems.

Option D is incorrect. Real-time monitoring can provide alerts on suspicious activities, but it doesn't provide the desired isolation.

Question 405. After a major outage, CloudTech Services is reviewing their disaster recovery strategy. The company found out that after restoring from backup, several applications did not function properly due to configuration discrepancies. What would be the best approach to ensure a successful recovery in the future?

- (A) Prioritize applications for backup based on their importance
- (B) Implement differential backups in addition to full backups
- (C) **Regularly conduct a full system recovery in a test environment**

(D) Use a third-party backup solution instead of an in-house solution

Explanation 405. Correct Answer: C. Regularly conduct a full system recovery in a test environment. By conducting a full system recovery in a test environment, CloudTech can simulate a real-world recovery scenario. This helps in identifying any discrepancies, configuration issues, or application dependencies that might be missed during regular backups, ensuring a successful recovery when it's critically needed.

Option A is incorrect. Prioritizing applications for backup based on their importance doesn't address the configuration discrepancies or interdependencies between applications.

Option B is incorrect. Implementing differential backups, while beneficial in capturing changes, does not address the configuration discrepancies found during the recovery.

Option D is incorrect. Using a third-party solution instead of an in-house solution does not inherently guarantee a successful recovery or address the specific issue of configuration discrepancies.

Question 406. GlobalBank has implemented a backup strategy where only the changes made since the last full backup are recorded. Considering the need to optimize storage and reduce backup times, the IT team performs this type of backup every day. What backup frequency and type is GlobalBank utilizing?

(A) Incremental Backup daily

- (B) Differential Backup weekly
- (C) Full Backup bi-weekly
- (D) Snapshot Backup daily

Explanation 406. Correct Answer: A. Incremental Backup

daily. GlobalBank captures only the changes made since the last full backup, which is characteristic of incremental backups.

Furthermore, they perform this type of backup every day, indicating a daily frequency.

Option B is incorrect. Differential backups capture the changes made since the last full backup but would cumulatively grow in size each time until the next full backup, unlike the incremental which resets with each backup.

Option C is incorrect. A full backup would involve backing up all the data, regardless of changes, and the scenario does not mention a bi-weekly frequency.

Option D is incorrect. Snapshot backups capture the state of a system at a particular point in time, but the scenario specifically mentions capturing changes since the last full backup.

Question 407. A company has recently deployed a new e-commerce application. The security team wants to ensure they can detect any unauthorized or malicious activities on the application. Which of the following would be the MOST effective way to achieve this goal?

- (A) Conduct a penetration test on the application
- (B) Install a firewall in front of the application
- (C) **Implement continuous monitoring of the**

application's logs and activities

(D) Provide training to users about secure browsing habits

Explanation 407. Correct Answer: C. Implement continuous monitoring of the application's logs and activities.

Continuous monitoring of an application's logs and activities allows the security team to detect and respond to any suspicious or unauthorized behavior in real-time. This ensures that potential threats can be identified and addressed promptly, enhancing the security posture of the application.

Option A is incorrect. While a penetration test can identify vulnerabilities in an application, it does not offer continuous monitoring or detection capabilities for ongoing malicious activities.

Option B is incorrect. While a firewall can provide a layer of security by filtering malicious traffic, it doesn't offer the granular insights or real-time monitoring needed to detect all unauthorized activities within an application.

Option D is incorrect. Training users about secure browsing habits is important but would not directly help in monitoring or detecting malicious activities on the e-commerce application.

Question 408. Sophia, a network administrator, is reviewing the logs from the company's Intrusion Detection System (IDS). She notices an increased amount of outbound traffic to an unfamiliar IP address. Upon deeper analysis, she found that the traffic consists of sensitive data being transferred. What type of malicious code might be responsible for this?

- (A) Ransomware
- (B) Adware
- (C) **Data Exfiltration Malware**
- (D) Keylogger

Explanation 408. Correct Answer: C. Data Exfiltration

Malware. Data Exfiltration Malware is designed to extract and transfer sensitive data from the target system to a location controlled by the attacker. The fact that sensitive data is being transferred to an unfamiliar IP address points to this type of malicious code.

Option A is incorrect. Ransomware is a type of malware that encrypts the victim's files and demands a ransom to restore access. While it might involve data theft, it's primarily known for encryption and ransom demands, not for transferring data outward.

Option B is incorrect. Adware is a type of software that displays unwanted ads on a user's computer. While it might be intrusive and unwanted, it doesn't typically exfiltrate data.

Option D is incorrect. A Keylogger is designed to record keystrokes on a computer and may capture sensitive data like passwords. However, the primary behavior of a keylogger is capturing keystrokes, not transferring large amounts of data outward.

Question 409. ExamsDigest Enterprises wants to streamline their permission assignments. They decide that rather than assigning permissions to each user individually, they will group

users based on departmental roles and then assign permissions to these groups. For example, all members of the “Marketing” role would have access to the marketing database. Which access control method is ExamsDigest Enterprises employing?

- (A) Rule-based access control
- (B) Mandatory Access Control (MAC)
- (C) Discretionary Access Control (DAC)
- (D) **Role-Based Access Control (RBAC)**

Explanation 409. Correct Answer: D. Role-Based Access Control (RBAC). RBAC involves grouping users based on roles (in this case, departments like “Marketing”) and then assigning permissions to these roles. Individuals are then placed into these roles, which determines their access. The scenario described by ExamsDigest Enterprises is a clear example of implementing RBAC.

Option A is incorrect. Rule-based access control often deals with predefined rules for access, commonly used in firewalls or routers, and is not about grouping users based on roles.

Option B is incorrect. MAC is more about classifying information and having users with the appropriate clearance levels. It doesn’t deal with departmental roles like the scenario mentioned.

Option C is incorrect. DAC allows resource owners to grant or deny permissions. It does not inherently involve assigning permissions based on roles or job functions.

Question 410. A security administrator is considering a cryptographic solution for protecting data in transit between two servers located in the same data center. The primary goal is to ensure speed and efficiency in encryption and decryption processes. Which type of encryption would best meet this requirement?

- (A) Asymmetric encryption using RSA
- (B) **Symmetric encryption using AES**
- (C) Hybrid encryption using a combination of RSA and AES
- (D) Asymmetric encryption using ECC

Explanation 410. Correct Answer: B. Symmetric encryption using AES. Symmetric encryption, such as AES, is typically faster and requires less computational resources than asymmetric encryption. This makes it suitable for scenarios where high-speed encryption and decryption are essential, like for data in transit between servers in a data center.

Option A is incorrect. Asymmetric encryption using RSA is more computationally intensive than symmetric encryption and may not be the most efficient for the given scenario.

Option C is incorrect. While hybrid encryption can provide a balance of security and speed, using only symmetric encryption (AES) is more efficient for the described use case.

Option D is incorrect. ECC, like RSA, is an asymmetric encryption method, which means it will typically be slower than symmetric methods like AES.

Question 411. A large e-commerce company is deploying a new online payment system. The Chief Information Security Officer (CISO) is concerned about the security of cryptographic keys and wants to ensure they are protected from potential theft or compromise. Which tool should the CISO implement to provide the HIGHEST level of security for these keys?

- (A) Password vault
- (B) Software-based key storage
- (C) **Hardware Security Module (HSM)**
- (D) Cloud-based encryption service

Explanation 411. Correct Answer: C. Hardware Security Module (HSM). A Hardware Security Module (HSM) is a specialized device specifically designed to manage, protect, and securely store cryptographic keys. It is built to be tamper-resistant and provides a high level of security, making it suitable for environments where the protection of cryptographic keys is of paramount importance, such as in an e-commerce payment system.

Option A is incorrect. A password vault is designed primarily for storing and managing passwords, not cryptographic keys used in payment systems.

Option B is incorrect. Software-based key storage solutions do not provide the same level of physical security that an HSM offers.

Option D is incorrect. While cloud-based encryption services can provide encryption capabilities, they might not offer the

same level of physical protection and control as an on-premises HSM.

Question 412. During a security audit, a company realized that a malicious actor was able to situate themselves on the network path, capturing TLS handshake messages between clients and the server. The attacker's goal is to weaken the encryption by influencing the cipher suite negotiation process. What type of network attack does this scenario depict?

- (A) ARP Poisoning
- (B) **Downgrade Attack**
- (C) SYN Flood
- (D) Ping of Death

Explanation 412. Correct Answer: B. Downgrade Attack. A Downgrade Attack occurs when an attacker interferes with the setup process (e.g., TLS handshake) to force two entities to settle on a less secure communication mode or encryption standard. In this case, by capturing and potentially altering the TLS handshake messages, the attacker is trying to make the client and server use a weaker cipher suite.

Option A is incorrect. ARP Poisoning is a type of attack where an attacker sends falsified ARP messages over a local area network to link the attacker's MAC address with the IP address of another node (such as the default gateway). This is a way to facilitate on-path attacks, but the scenario describes influencing the cipher suite negotiation, which is a Downgrade Attack.

Option C is incorrect. SYN Flood is a form of denial-of-service attack in which an attacker sends a sequence of SYN

requests to a target's system in an attempt to consume server resources. It does not relate to capturing TLS handshake messages.

Option D is incorrect. Ping of Death is an old attack where malicious parties send malformed or oversized ping packets to crash the target system. It doesn't involve capturing or influencing the TLS handshake process.

Question 413. A software developer wants to store user passwords in a way that even if the database is compromised, attackers would not be able to retrieve the original passwords. What technique should the developer use to achieve this?

- (A) Symmetric encryption
- (B) Digital signing
- (C) **Hashing**
- (D) Steganography

Explanation 413. Correct Answer: C. Hashing. Hashing is a technique that takes an input (or 'message') and returns a fixed-size string of bytes, usually in the form of a digest. The output should ideally be unique (within reason) for every different input. It's often used for storing passwords because even a tiny change in input will produce a dramatically different output, and it's computationally hard to reverse the process.

Option A is incorrect. Symmetric encryption uses the same key for both encryption and decryption. If an attacker gains access to the encryption key, they can decrypt any encrypted data.

Option B is incorrect. Digital signing is used to verify the integrity and authenticity of a message but does not hide the original content.

Option D is incorrect. Steganography involves hiding information within other information, which isn't related to securely storing passwords.

Question 414. A company's IT department notices a sharp increase in account lockouts over the past two days, especially during non-business hours. While some accounts are from various departments, a majority are from the finance team. Which of the following is the MOST plausible explanation for these lockouts?

- (A) Scheduled maintenance by the IT department
- (B) Employees are sharing passwords within the finance team
- (C) **An attacker is trying to gain unauthorized access**
- (D) A recent password policy change requiring more frequent changes

Explanation 414. Correct Answer: C. An attacker is trying to gain unauthorized access. A sudden increase in account lockouts, especially during non-business hours, indicates suspicious activity. The targeted nature of the lockouts, especially on sensitive departments like finance, suggests an attacker might be attempting unauthorized access.

Option A is incorrect. Scheduled maintenance would typically be communicated in advance, and it's unlikely to cause a sharp increase in account lockouts.

Option B is incorrect. While employees sharing passwords is a security concern, it would not typically result in a surge of account lockouts, especially during non-business hours.

Option D is incorrect. A password policy change might result in some increased lockouts, but the targeted nature of the lockouts (majority from finance) and their occurrence during non-business hours make this option less likely.

Question 415. Carlos is responsible for managing IT services for a university. The university has numerous departments, each with its subdomain, like arts.university.com, science.university.com, and sports.university.com. Carlos wants a solution that ensures HTTPS security while being cost-effective. However, he's wary of potential risks. What might be a drawback of using a Wildcard Certificate for the university's subdomains?

- (A) It can secure only one subdomain
- (B) **If compromised, all subdomains are at risk**
- (C) It only validates the domain ownership, not the organization's identity
- (D) It's the most expensive certificate available

Explanation 415. Correct Answer: B. If compromised, all subdomains are at risk. The primary concern with a Wildcard Certificate is that if its private key is compromised, it jeopardizes the security of all associated subdomains. This poses a significant risk since the exposure of a single key could lead to potential attacks or misuse across all subdomains.

Option A is incorrect. A Wildcard Certificate can secure multiple subdomains under a single domain.

Option C is incorrect. While true for Domain Validated (DV) certificates, Wildcard Certificates can also be available with Organization Validation (OV), ensuring organizational identity.

Option D is incorrect. Wildcard Certificates aren't necessarily the most expensive. The cost varies based on the level of validation and the issuing authority.

Question 416. SecureData Inc., a financial firm, recently experienced a system crash and needed to restore their database. While they had a full backup from the previous week, they realized that several days of transactions were missing. To prevent such data loss in the future, which backup strategy involving recording transactions can SecureData implement?

- (A) Implement differential backups
- (B) Use snapshot backups every hour
- (C) **Enable database journaling**
- (D) Configure RAID 5 for their storage

Explanation 416. Correct Answer: C. Enable database journaling. Journaling involves keeping a log or 'journal' of every transaction or change that happens. If there's a crash, the system can be restored to the last backup and then use the journal to replay each transaction, thus preventing data loss.

Option A is incorrect. Differential backups capture changes since the last full backup, but they don't record every transaction in real-time like journaling.

Option B is incorrect. While hourly snapshot backups would reduce the potential data loss window, they still don't capture every transaction in real-time.

Option D is incorrect. RAID 5 offers redundancy and can protect against a disk failure, but it doesn't capture and record every database transaction like journaling.

Question 417. A company has set up its firewall to allow web traffic through port 80 and port 443, while denying all other traffic by default. This setup is an example of which type of access control?

- (A) Role-Based Access Control (RBAC)
- (B) Mandatory Access Control (MAC)
- (C) Discretionary Access Control (DAC)
- (D) **Rule-Based Access Control (RAC)**

Explanation 417. Correct Answer: D. Rule-Based Access Control (RAC). Rule-Based Access Control (RAC) operates based on predefined rules set by administrators. In the scenario described, the firewall is using rules to allow traffic on certain ports (80 and 443) while denying all others, making this a clear example of RAC.

Option A is incorrect. RBAC assigns permissions based on roles within an organization. Firewall rules are not typically assigned based on user roles.

Option B is incorrect. MAC involves classifying information and matching user clearance levels to these classifications. It is unrelated to firewall rule settings.

Option C is incorrect. DAC allows resource owners to specify who can access their resources. Firewall rule settings don't operate based on individual discretion.

Question 418. During a routine security assessment, Jake, a penetration tester, discovers that by modifying a configuration file located in a public directory, he can assign himself administrative privileges in the application. What type of vulnerability is Jake exploiting?

- (A) Cross-Site Scripting (XSS)
- (B) **Privilege Escalation**
- (C) SQL Injection
- (D) Insecure Direct Object Reference (IDOR)

Explanation 418. Correct Answer: B. Privilege Escalation.

Privilege escalation occurs when a user increases their privileges beyond what was originally granted to them, allowing them to perform actions that they should not be allowed to. In this scenario, Jake is elevating his privileges in the application by modifying a configuration file, indicating a privilege escalation vulnerability.

Option A is incorrect. Cross-Site Scripting (XSS) involves an attacker injecting malicious scripts into web content viewed by other users. This scenario does not relate to injecting scripts.

Option C is incorrect. SQL Injection vulnerabilities allow attackers to manipulate or query a database directly through input fields. The scenario does not indicate any interaction with a database.

Option D is incorrect. Insecure Direct Object Reference (IDOR) vulnerabilities occur when an application allows access to objects based on user-supplied input. While the scenario involves accessing a file, it is the act of elevating privileges that is the primary concern.

Question 419. A school wants to prevent its students from accessing inappropriate websites during class hours. The IT department decides to implement a solution that blocks requests to specific domain names associated with inappropriate content. Which of the following security solutions would best address this need?

- (A) Firewall filtering based on IP addresses
- (B) Intrusion Detection System monitoring
- (C) Virtual Private Network (VPN) enforcement
- (D) **DNS filtering with a blacklist**

Explanation 419. Correct Answer: D. DNS filtering with a blacklist. DNS filtering is a technique that can be used to prevent users from accessing specific websites by blocking requests to certain domain names. A blacklist can be created to list the domain names associated with inappropriate content, and when users try to access these sites, the DNS filter will not resolve the domain name, thereby preventing access.

Option A is incorrect. While firewalls can block traffic based on IP addresses, this method is not as effective for blocking specific domain names, especially when a domain can have multiple IP addresses or if the IPs can change.

Option B is incorrect. Intrusion Detection Systems (IDS) are primarily used for detecting and alerting on malicious activities but not for blocking access to specific domain names.

Option C is incorrect. VPNs are used to create a secure communication channel and are not inherently designed to block domain name resolutions.

Question 420. A financial firm has just experienced a cyber attack, and the IT team identified a piece of malware that evaded their traditional antivirus solutions. The CISO now wants to not only detect but also be able to analyze and respond to such advanced threats in real-time. Which solution should the firm consider implementing?

- (A) Vulnerability Scanner
- (B) Intrusion Prevention System (IPS)
- (C) **Endpoint Detection and Response (EDR)**
- (D) Patch Management System

Explanation 420. Correct Answer: C. Endpoint Detection and Response (EDR). Endpoint Detection and Response (EDR) provides real-time monitoring and analysis of endpoint events, allowing an organization to detect, investigate, and respond to potential security threats. EDR tools can identify behaviors that might indicate advanced threats that evade traditional antivirus solutions.

Option A is incorrect. Vulnerability Scanners are used to identify vulnerabilities in a system or network but do not provide real-time monitoring and response capabilities for threats.

Option B is incorrect. Intrusion Prevention Systems (IPS) monitor network traffic to prevent potential threats, but they might not provide in-depth analysis and response at the endpoint level like EDR solutions do.

Option D is incorrect. Patch Management Systems are used to manage the distribution and installation of software updates but do not offer real-time threat detection and response.

Question 421. During a routine audit of the corporate servers, the system administrator discovers that a week's worth of security logs are missing from one of the key application servers. Which of the following is the MOST likely reason for this occurrence?

- (A) The logging service experienced a malfunction
- (B) There was insufficient storage space for the logs
- (C) **A malware attack aimed to erase traces of intrusion**
- (D) The time zone setting was incorrectly configured

Explanation 421. Correct Answer: C. A malware attack aimed to erase traces of intrusion. One of the primary tactics attackers use after gaining unauthorized access is to cover their tracks. Deleting or altering logs is a common method used to avoid detection and prevent any trace of malicious activity.

Option A is incorrect. While it's possible for the logging service to malfunction, it's less likely for it to result in a specific week's worth of logs being missing, without affecting other time periods.

Option B is incorrect. Insufficient storage space can cause newer logs to overwrite older ones, but it would typically not result in a discrete chunk of logs, such as an entire week, to be missing.

Option D is incorrect. A misconfigured time zone setting might cause timestamp discrepancies in logs, but it wouldn't cause logs to be missing.

Question 422. A financial company is designing a new system that needs to ensure data is accessed based on classifications and clearance levels of the users. Which of the following access control models BEST fits this requirement?

- (A) Role-Based Access Control (RBAC)
- (B) Discretionary Access Control (DAC)
- (C) **Mandatory Access Control (MAC)**
- (D) Attribute-Based Access Control (ABAC)

Explanation 422. Correct Answer: C. Mandatory Access Control (MAC). MAC is based on the classification of information and the clearance level of users. In a MAC model, the operating system constrains the ability of a subject or initiator to access or perform some sort of operation on an object or target. In this scenario, where data is classified and users are given clearance levels, MAC is the most suitable model.

Option A is incorrect. Role-Based Access Control (RBAC) assigns permissions to specific roles in an organization. Users are then assigned to roles. While useful in many contexts, it doesn't focus on classifications and clearance levels.

Option B is incorrect. Discretionary Access Control (DAC) allows the owner of the resource to specify who can access it. It's more flexible but less restrictive than MAC.

Option D is incorrect. Attribute-Based Access Control (ABAC) uses policies to determine access, based on attributes of users, the environment, and the resource itself. While it can be used in scenarios with classifications and clearances, it's not as strictly based on these factors as MAC.

Question 423. TechSolutions Inc., a rapidly growing startup, is expanding its workforce to meet its customer demands. As part of this expansion, they need to ensure their IT infrastructure can accommodate the influx of new employees without compromising performance or security. Which of the following should be TechSolutions' primary focus during this expansion phase?

- (A) Adopting a Zero Trust Network Architecture
- (B) Increasing the frequency of vulnerability assessments
- (C) **Implementing capacity planning**
- (D) Deploying additional firewalls and intrusion detection systems

Explanation 423. Correct Answer: C. Implementing capacity planning. Capacity planning ensures that an organization's infrastructure, technology, and people are scaled appropriately to meet growth and performance needs. In the scenario, with an influx of new employees, ensuring that the IT infrastructure can handle the increased demand is crucial.

Option A is incorrect. While adopting a Zero Trust Network Architecture might enhance security, it doesn't address the need to scale resources to accommodate new employees.

Option B is incorrect. Vulnerability assessments are crucial for security, but they don't directly address the infrastructure's ability to handle growth.

Option D is incorrect. While firewalls and IDS can improve security, they don't directly address the organization's capacity to handle more employees

Question 424. Emily, a cybersecurity analyst, has been tasked with gathering preliminary information about a target organization without directly interacting with its systems. She decides to collect data from third-party sources, search engines, public records, and other online platforms without sending any packets to the target. Which phase of penetration testing is Emily currently engaged in?

- (A) Active reconnaissance
- (B) **Passive reconnaissance**
- (C) Vulnerability scanning
- (D) Threat hunting

Explanation 424. Correct Answer: B. Passive reconnaissance. Passive reconnaissance is the initial phase in which the penetration tester collects information about the target without directly engaging with or alerting the target. Emily's approach of gathering data from third-party sources without sending packets or interacting directly with the target's systems is in line with the characteristics of passive reconnaissance.

Option A is incorrect. Active reconnaissance involves directly interacting with the target systems, often sending packets or probes, which can potentially be detected by the target.

Option C is incorrect. Vulnerability scanning is a step further where specific tools are used to identify vulnerabilities in a system. It is more direct than passive reconnaissance.

Option D is incorrect. Threat hunting is a proactive approach to finding malicious activities within a system rather than gathering information about a target system.

Question 425. During the setup of a secure communication channel, Alice and Bob need to agree upon a shared secret key without sending the key directly to each other, as they fear eavesdropping. Which protocol would best facilitate this requirement?

- (A) RSA
- (B) HMAC
- (C) **Diffie-Hellman**
- (D) AES

Explanation 425. Correct Answer: C. Diffie-Hellman. The Diffie-Hellman key exchange protocol allows two parties to each generate public and private key pairs, exchange the public keys, and then derive a shared secret key. This secret key can then be used for symmetric encryption. The beauty of this protocol is that the shared secret can be derived without directly sending it over the communication channel, preventing eavesdroppers from obtaining the secret key directly.

Option A is incorrect. RSA is an asymmetric encryption method, not a key exchange protocol.

Option B is incorrect. HMAC is a specific type of message authentication code that involves hashing and is not used for key exchange.

Option D is incorrect. AES is a symmetric encryption algorithm and does not offer a key exchange mechanism.

Question 426. A company plans to upgrade its email server to ensure that email transmission between their mail server and client applications is encrypted. Which of the following protocols would be the most appropriate for this purpose?

- (A) HTTP
- (B) FTP
- (C) IMAP over SSL/TLS
- (D) SNMP

Explanation 426. Correct Answer: C. IMAP over SSL/TLS. IMAP over SSL/TLS (commonly known as IMAPS) is a protocol used by email clients to retrieve messages from a mail server over a secure channel. The use of SSL/TLS provides encryption for the transmitted data, ensuring confidentiality of the email transmission.

Option A is incorrect. HTTP is a protocol for transferring web content and does not provide encryption by default. Furthermore, it's not designed for email transmission.

Option B is incorrect. FTP is a protocol for transferring files and does not provide secure email transmission capabilities.

Option C is incorrect. SNMP (Simple Network Management Protocol) is used for network management and monitoring, not for email transmission.

Question 427. A medium-sized company has just deployed a new file server for the HR department. They want to ensure that only HR employees can view and edit HR-specific documents, while the IT department should only be able to perform system maintenance tasks. What should the company implement to achieve this requirement?

- (A) Install a firewall between the HR and IT departments
- (B) Implement an Access Control List (ACL) for the file server**
- (C) Enforce a strong password policy for the HR department
- (D) Enable full disk encryption on the file server

Explanation 427. Correct Answer: B. Implement an Access Control List (ACL) for the file server. Access Control Lists (ACLs) define who can access a resource and what they can do with it once accessed. By setting up an ACL for the file server, the company can precisely define the permissions for HR and IT departments, ensuring that only authorized users have the right level of access to the data.

Option A is incorrect. Installing a firewall would limit network traffic between departments but would not provide granular access control to files on the server.

Option C is incorrect. While a strong password policy is essential for security, it doesn't differentiate access between HR and IT or control what users can do once they access the server.

Option D is incorrect. Full disk encryption protects data at rest, but it does not provide differentiated access to specific files or directories based on user roles.

Question 428. Carla, a security analyst, receives an alert that one of the company's server certificates may have been exposed in a recent data breach. What is the most immediate action Carla should take to ensure that the exposed certificate cannot be used maliciously?

- (A) Request a new certificate from the CA
- (B) Update the company firewall rules
- (C) **Add the certificate to the Certificate revocation list (CRL)**
- (D) Perform a vulnerability assessment on the server

Explanation 428. Correct Answer: C. Add the certificate to the Certificate revocation list (CRL). If a certificate is believed to be compromised, the most immediate action is to revoke it. This is done by adding the certificate to the Certificate revocation list (CRL). Systems and applications that check the CRL before establishing secure communications will then know not to trust the compromised certificate.

Option A is incorrect. While requesting a new certificate may be necessary after revoking the compromised one, the immediate action should be revoking the potentially compromised certificate.

Option B is incorrect. Updating firewall rules, while essential for many security scenarios, doesn't directly address the misuse of a potentially exposed certificate.

Option D is incorrect. A vulnerability assessment is a broader action to identify weaknesses in the system. While valuable, it doesn't directly address the issue of the compromised certificate.

Question 429. DataFin, a financial analytics firm, experienced a minor fire incident in one of its server rooms. Fortunately, they had backups stored in another wing of the building, allowing for quick data recovery. However, management realizes that in a major disaster, both primary and backup data might be destroyed. To address this, which backup strategy should DataFin consider?

- (A) Mirror Backup
- (B) Local Storage Backup
- (C) Incremental Backup
- (D) **Offsite Backup**

Explanation 429. Correct Answer: D. Offsite Backup. Offsite Backup involves storing backup data in a different geographical location from the primary data. This ensures that even if a disaster impacts the primary location, the backup remains safe and can be used for recovery.

Option A is incorrect. Mirror Backup refers to a backup that is an exact copy of the source data. It doesn't specify the geographic location of the backup.

Option B is incorrect. Local Storage Backup typically means backups are stored within the same physical premises or close vicinity of the primary data, which wouldn't address DataFin's concern of potential data loss in a major disaster.

Option C is incorrect. Incremental Backup involves backing up only the data that has changed since the last backup, regardless of where it's stored. It doesn't address the concern of geographic separation.

Question 430. An online retailer is considering various methods to protect its customers' credit card information. Instead of storing the actual credit card numbers in their database, they opt for a solution that replaces the numbers with unrelated, random values. What is this method called?

- (A) Symmetric encryption
- (B) Digital watermarking
- (C) Hashing
- (D) **Tokenization**

Explanation 430. Correct Answer: D. Tokenization.

Tokenization is a method where sensitive data is replaced with non-sensitive substitutes, referred to as "tokens". These tokens act as references to the original data but don't contain the actual sensitive data, making it a preferred method for protecting credit card information in many retail environments.

Option A is incorrect. Symmetric encryption is a method of encrypting data using a single key for both encryption and decryption. It changes the original data into a ciphered format but doesn't replace it with random values as tokenization does.

Option B is incorrect. Digital watermarking embeds data into a digital signal, primarily for asserting rights or ownership and not for replacing sensitive data with random values.

Option C is incorrect. Hashing converts input data into a fixed-length string of characters, which is typically a hash code. It doesn't produce a random value that can be used as a reference back to the original data.

Question 431. The IT team at TechnoCorp has noticed a consistent pattern over the last week where a particular server's CPU usage spikes to 100% between 2:00 AM and 4:00 AM, a time when there's typically minimal user activity. What could be the MOST probable reason for this?

- (A) The server is automatically updating its software
- (B) An employee is running a heavy computational task
- (C) The server is undergoing a DDoS attack
- (D) **Malware is performing cryptomining activities**

Explanation 431. Correct Answer: D. Malware is performing cryptomining activities. Cryptomining malware often causes significant resource consumption, especially CPU usage. Attackers frequently schedule such activities during off-peak hours to reduce the chance of detection. Given the consistent pattern of high CPU usage during off-hours, cryptomining malware is a probable cause.

Option A is incorrect. While software updates can cause resource consumption, they typically don't result in consistent, prolonged 100% CPU usage over multiple days.

Option B is incorrect. Though it's possible an employee might be running a heavy task, the consistent pattern during odd hours makes it less likely compared to malicious activities.

Option C is incorrect. While a DDoS attack can cause resource consumption, it wouldn't specifically target CPU usage consistently during the same timeframe every night.

Question 432. A journalist wants to send a confidential message to her editor without raising suspicion. Instead of sending a coded or encrypted text, she embeds the message within a harmless-looking photograph. What method is she employing to keep the message concealed?

- (A) Digital signature
- (B) Tunneling
- (C) **Steganography**
- (D) Chaining

Explanation 432. Correct Answer: C. Steganography.

Steganography is a technique used to conceal data within another piece of data. In this scenario, the journalist is embedding a confidential message within a photograph, making it look harmless and unsuspecting.

Option A is incorrect. A digital signature is used to verify the authenticity and integrity of a message or document. It doesn't hide information within another piece of data.

Option B is incorrect. Tunneling is a method used to encapsulate one protocol within another, typically used in VPNs to transport data over a public network.

Option D is incorrect. Chaining in the context of cryptography often refers to modes of operation like Cipher Block Chaining (CBC). It doesn't involve hiding data within other data.

Question 433. Ella, a security analyst, is reviewing the logs of a web application and notices that an attacker attempted to use the following input in a login form: ' OR '1'='1' --. This input was used in an effort to manipulate the application's backend database. What type of injection attack is this an example of?

- (A) XML Injection
- (B) Command Injection
- (C) **SQL Injection**
- (D) LDAP Injection

Explanation 433. Correct Answer: C. SQL Injection. The input ' OR '1'='1' -- is a classic example of an SQL injection attack. Attackers use this technique to manipulate SQL queries in applications that do not properly validate user input, potentially allowing unauthorized access or data retrieval.

Option A is incorrect. XML Injection targets applications that parse XML input. The payload mentioned in the scenario is not related to XML structures.

Option B is incorrect. Command Injection is when an attacker attempts to execute arbitrary commands on a host operating system. The given input is not an OS command.

Option D is incorrect. LDAP Injection targets applications that construct LDAP statements based on user input. The given payload is not structured for LDAP queries.

Question 434. During a security audit, it was found that an application was using plain hashes for storing passwords. The security team recommended a method that involves using the original password along with a salt and then rehashing it multiple times. What is this method known as?

- (A) Key clustering
- (B) Rainbow table prevention
- (C) Key rotation
- (D) **Key stretching**

Explanation 434. Correct Answer: D. Key stretching. Key stretching refers to the process of taking a password and, usually in combination with a salt, hashing it multiple times. This repeated hashing process makes brute-force attacks more time-consuming and difficult because the attacker has to not only guess the password but also apply the hashing function the same number of times the original process used.

Option A is incorrect. Key clustering pertains to different keys producing the same ciphertext from the same plaintext, which is not relevant to the described scenario.

Option B is incorrect. While using salts can prevent the effective use of rainbow tables, the act of rehashing passwords multiple times is not specifically called “rainbow table prevention.”

Option C is incorrect. Key rotation involves periodically changing cryptographic keys. It does not relate to hashing passwords multiple times.

Question 435. A university's IT department provides access to its student records for training purposes to new hires. To protect student identities, they replace the real names and social security numbers with fictitious ones while maintaining the database's original format. Which technique is the IT department utilizing?

- (A) Digital signing
- (B) **Data masking**
- (C) Steganography
- (D) Data deduplication

Explanation 435. Correct Answer: B. Data masking. Data masking protects the data subject's data privacy by obscuring specific data within a database, making the data unreadable and unusable, especially in non-production environments. It is commonly used for testing and development purposes.

Option A is incorrect. Digital signing involves using a digital signature to prove the authenticity and integrity of data.

Option C is incorrect. Steganography involves hiding information within other information, such as embedding text within images, making it undetectable.

Option D is incorrect. Data deduplication is the process of eliminating duplicate copies of repeating data to save storage space.

Question 436. StreamNet, a popular online streaming service, is planning to launch in three new countries. They anticipate a substantial increase in users and concurrent streams. To ensure

that the service remains uninterrupted and provides a seamless experience to new users, which action related to capacity planning should StreamNet prioritize?

- (A) Investing in content encryption and DRM
- (B) Increasing marketing and promotional activities in the new countries
- (C) Implementing stronger user authentication methods
- (D) **Expanding and optimizing their infrastructure to handle the projected growth**

Explanation 436. Correct Answer: D. Expanding and optimizing their infrastructure to handle the projected growth. Infrastructure capacity planning will allow StreamNet to predict the necessary resources required and make the needed upgrades or adjustments to their servers, networks, storage, and other infrastructure components. This ensures a smooth user experience even with the influx of new users.

Option A is incorrect. While content encryption and DRM (Digital Rights Management) are essential for protecting content, they don't address the infrastructure capacity needed to handle more users.

Option B is incorrect. Marketing and promotional activities can attract users but don't directly impact the infrastructure's capacity to support those users.

Option C is incorrect. Stronger authentication methods can improve security but don't address the capacity or scalability of the infrastructure.

Question 437. The IT department of an e-commerce company is configuring access controls for a new online product inventory system. They want the sales team to update the inventory levels and product details but don't want them to access financial data stored in the same system. Which access control principle is the IT department applying?

- (A) Least Privilege
- (B) **Role-Based Access Control (RBAC)**
- (C) Mandatory Access Control (MAC)
- (D) User-Based Access Control (UBAC)

Explanation 437. Correct Answer: B. Role-Based Access Control (RBAC). Role-Based Access Control (RBAC) assigns permissions based on roles within an organization. Individuals are then assigned roles, and the permissions associated with that role determine what they can and cannot access. In this scenario, the sales team would be given a role that allows them to update inventory but restricts access to financial data.

Option A is incorrect. While the principle of Least Privilege dictates that users should only be given the minimal necessary access to perform their tasks, the scenario specifically focuses on roles (sales team) and the permissions associated with that role, which aligns more with RBAC.

Option C is incorrect. Mandatory Access Control (MAC) uses labels (e.g., classification levels) to determine access. It's more rigid than RBAC and isn't described in the given scenario.

Option D is incorrect. User-Based Access Control (UBAC) assigns permissions directly to each user, rather than based on

their role. The scenario emphasizes role-based permissions, making RBAC the appropriate choice.

Question 438. The IT department of XYZ Corp noticed that server logs are recording user login attempts during non-business hours, specifically between 2:00 AM and 3:00 AM, a time when no scheduled tasks or backups are set to run. Which of the following is the MOST plausible explanation for this unusual activity?

- (A) The company's employees are working overtime
- (B) There might be a time zone misconfiguration on the server
- (C) **An unauthorized user is trying to gain access to the server**
- (D) The server is automatically installing security patches

Explanation 438. Correct Answer: C. An unauthorized user is trying to gain access to the server. Out-of-cycle logging that occurs during unusual hours, especially when no scheduled tasks are set, can be a significant indicator of malicious activity. In this scenario, the logging of user login attempts during non-business hours suggests an unauthorized user might be attempting access.

Option A is incorrect. While employees might occasionally work overtime, regular login attempts specifically between 2:00 AM and 3:00 AM are suspicious.

Option B is incorrect. A time zone misconfiguration might cause time discrepancies in logs, but it wouldn't result in repeated login attempts.

Option D is incorrect. Automatic security patch installations wouldn't result in user login attempts.

Question 439. A financial institution processes thousands of credit card transactions daily. To ensure the security and integrity of these transactions, the security officer wants to employ a solution that will safely manage and store cryptographic keys. Which of the following would be the MOST suitable solution?

- (A) Trusted Platform Module (TPM)
- (B) Full Disk Encryption (FDE)
- (C) **Hardware Security Module (HSM)**
- (D) Software Key Repository

Explanation 439. Correct Answer: C. Hardware Security Module (HSM). Hardware Security Modules (HSMs) are physical devices specifically designed to manage, process, and store cryptographic keys. They provide a high level of protection against both physical and logical attacks and are commonly used by financial institutions to ensure the security of high-value transactions.

Option A is incorrect. While TPMs provide hardware-level security for individual devices, they are not designed for the high-capacity cryptographic needs of an institution processing numerous transactions.

Option B is incorrect. Full Disk Encryption (FDE) secures data at rest on a hard drive but doesn't specifically manage cryptographic keys used in transaction processing.

Option D is incorrect. While a software key repository can store cryptographic keys, it lacks the same level of physical and logical protection provided by an HSM.

Question 440. XYZ Corp recently faced a ransomware attack that encrypted critical data files. The company's IT team was unable to decrypt the files but had a recent backup available. However, when they tried to restore the data, they found out the backup was corrupted. Which of the following best practices would have helped XYZ Corp in ensuring the integrity of their backups?

- (A) **Regularly testing backup restoration processes**
- (B) Storing backups in the same directory as original files
- (C) Increasing the frequency of backups to every hour
- (D) Encrypting backups with a strong encryption algorithm

Explanation 440. Correct Answer: A. Regularly testing backup restoration processes. By regularly testing the restoration process from backups, organizations can identify and correct any issues with the backup files or processes before they are needed in a critical recovery situation.

Option B is incorrect. Storing backups in the same directory as the original files increases the risk of both the original and backup files being compromised or corrupted simultaneously.

Option C is incorrect. While increasing the frequency of backups can reduce data loss, it doesn't address the integrity or validity of the backups themselves.

Option D is incorrect. While encrypting backups provides security against unauthorized access, it doesn't ensure the integrity or usability of the backup.

Question 441. An e-commerce company stores millions of customer transaction records in their primary database. They have decided to enhance their security posture by applying encryption to protect sensitive data. However, they don't want to encrypt the entire server storage, just the data within the database. Which encryption approach should the company adopt to meet their objective?

- (A) Full-disk Encryption
- (B) File-level Encryption
- (C) Volume-level Encryption
- (D) **Database-level Encryption**

Explanation 441. Correct Answer: D. Database-level Encryption. Database-level Encryption provides encryption specifically for data within a database. It ensures that the data remains encrypted even when backed up, replicated, or moved. This approach is ideal for the e-commerce company as it focuses on encrypting the sensitive transaction records without affecting other data on the server.

Option A is incorrect. Full-disk Encryption would encrypt the entire server's storage, which may not be required by the company.

Option B is incorrect. File-level Encryption would require encrypting individual files, which may not be efficient for a database with millions of records.

Option C is incorrect. Volume-level Encryption encrypts specific volumes or logical drives, not just the database data.

Question 442. A database administrator is concerned about identical hashes being produced for users who select the same password. To mitigate this risk, what cryptographic technique should the administrator implement?

- (A) Digital signature
- (B) **Salting**
- (C) Key stretching
- (D) Symmetric encryption

Explanation 442. Correct Answer: B. Salting. Salting involves adding a random value to a password before hashing it. This ensures that even if two users have the same password, their hashes will be different because of the unique salts. This makes it difficult for attackers to use precomputed tables (like rainbow tables) to match hashes to possible plaintext passwords.

Option A is incorrect. Digital signatures are primarily used to ensure the authenticity and integrity of a message or data, not for hashing passwords.

Option C is incorrect. Key stretching involves repeating the hashing process multiple times to make brute-force attacks more challenging, but it doesn't address the problem of identical hashes for identical passwords.

Option D is incorrect. Symmetric encryption uses the same key for both encryption and decryption and isn't related to the scenario of producing unique hashes for passwords.

Question 443. After a recent data breach, a multinational corporation is evaluating its cryptographic practices. The Chief Security Officer (CSO) determines that the manual management of cryptographic keys has become too complex due to the scale of the operations. Which tool would BEST address the CSO's concern while ensuring robust security practices?

- (A) Password Management System
- (B) Secure File Transfer Protocol (SFTP)
- (C) Trusted Platform Module (TPM)
- (D) **Key Management System (KMS)**

Explanation 443. Correct Answer: D. Key Management System (KMS). A Key Management System (KMS) is specifically designed to handle the generation, distribution, rotation, and retirement of cryptographic keys in a centralized and automated manner. For large organizations, using a KMS streamlines and secures the complex task of key management.

Option A is incorrect. While a Password Management System helps in handling and storing passwords, it does not provide comprehensive features needed for cryptographic key management.

Option B is incorrect. SFTP is a protocol for securely transferring files over a network, not for managing cryptographic keys.

Option C is incorrect. While TPM provides hardware-level security for individual devices, it is not meant for enterprise-wide key management.

Question 444. After a security incident, a forensic investigation revealed that a compromised internal workstation was communicating with a known malicious IP address. To prevent further communication, the security team decided to take immediate action. Which of the following is the BEST immediate action to ensure the workstation cannot communicate with that IP?

- (A) **Implement a block rule on the web filter for the IP address**
- (B) Disable the network port of the compromised workstation
- (C) Use a honeypot to divert the traffic from the malicious
- (D) Update the firewall's firmware

Explanation 444. Correct Answer: A. Implement a block rule on the web filter for the IP address. By implementing a block rule specifically for the known malicious IP address on the web filter, any attempt to communicate with that IP would be stopped, effectively preventing further malicious communications.

Option B is incorrect. Disabling the network port of the compromised workstation would disconnect the machine from the network, but it wouldn't specifically prevent communication with the malicious IP if the port were to be re-enabled.

Option C is incorrect. While honeypots can be used to divert or study attacker behavior, they are not the most direct way to block communication with a known malicious IP address.

Option D is incorrect. Updating the firewall's firmware is a general maintenance task and does not specifically address blocking communications with the known malicious IP.

Question 445. Jennifer, an IT administrator, is asked to onboard a new remote employee for a sales role. Which of the following is the BEST approach for provisioning the user account?

- (A) Assign the new user the same access privileges as the CEO because they might require all resources
- (B) Provide the new user with administrative rights to ensure they can install and configure any needed software
- (C) **Use the access privileges from a template of a salesperson to provide the required resources**
- (D) Allow the new user to decide and self-select the necessary access based on their job role

Explanation 445. Correct Answer: C. Use the access privileges from a template of a salesperson to provide the required resources. Provisioning users based on role templates ensures that users have just the access they need, adhering to the principle of least privilege.

Option A is incorrect. This goes against the principle of least privilege and can introduce significant security risks.

Option B is incorrect. Giving administrative rights to employees without a proper need can expose the organization to unnecessary risks.

Option D is incorrect. Users should not self-select access rights as they might not be aware of potential security implications.

Question 446. The IT department of a large organization receives reports from employees that they are unable to access certain resources on the network. Upon investigation, the IT department discovers that the Access Control List (ACL) settings have been recently modified. Which of the following would be the PRIMARY reason to review and modify the ACL settings?

- (A) To balance the network load
- (B) To update the organization's firewall rules.
- (C) **To ensure appropriate access rights to resources**
- (D) To update the organization's password policy

Explanation 446. Correct Answer: C. To ensure appropriate access rights to resources. ACLs are essential tools in determining who has access to which resources within a network or system. Regularly reviewing and modifying the ACL settings ensures that users have the appropriate access rights, preventing unauthorized access and ensuring that authorized users can access the resources they need.

Option A is incorrect. While network load balancing is crucial, it is not directly related to ACLs. ACLs focus on access control, not traffic distribution.

Option B is incorrect. Firewall rules are different from ACLs. While they can work together, firewall rules primarily focus on

allowing or blocking network traffic, while ACLs determine access permissions to resources.

Option D is incorrect. While updating the organization's password policy is a vital security measure, it is not related to ACLs, which control access to resources based on user or group permissions.

Question 447. TechWorld Corp is concerned about cybercriminals sending emails that appear to come from its domain to deceive its clients. The company wants to implement a solution that would allow receiving email servers to validate that an email claiming to come from TechWorld Corp's domain indeed originates from an approved server. Which of the following should the company implement?

- (A) SMTP authentication
- (B) **DKIM**
- (C) POP3 over SSL
- (D) S/MIME

Explanation 447. Correct Answer: B. DKIM. DomainKeys Identified Mail (DKIM) is a method used to authenticate the origin and integrity of an email. With DKIM, a digital signature is added to the headers of outgoing emails. Receiving email servers then use this signature to validate the email by checking it against the sending domain's public key, which is published in the DNS records.

Option A is incorrect. SMTP authentication ensures that users provide valid credentials before they can send emails through a

server, but it doesn't validate the domain of the sender to the receiver.

Option C is incorrect. POP3 over SSL (Secure Sockets Layer) is about securely retrieving email messages from a server. It doesn't provide a way to authenticate the sender's domain.

Option D is incorrect. S/MIME (Secure/Multipurpose Internet Mail Extensions) is used to encrypt and sign email messages. While it ensures the integrity and confidentiality of the email content, it does not validate the sender's domain to the recipient.

Question 448. A cloud-based collaboration tool used by a company displays a warning to a user stating, "You are logged in from two locations." However, the user has only one active session on their workstation. What should be the primary concern for the security team?

- (A) The user might be using multiple devices
- (B) There's a potential misconfiguration in the tool's settings
- (C) The collaboration tool is facing an outage
- (D) **There might be unauthorized access to the user's account**

Explanation 448. Correct Answer: D. There might be unauthorized access to the user's account. Warnings of concurrent sessions, especially when the user is certain they're using only one device, are red flags for potential unauthorized access. The security team should treat this as a priority and investigate for signs of a breach.

Option A is incorrect. While users often use multiple devices, the scenario mentions the user is certain they have only one active session, making this option unlikely.

Option B is incorrect. While misconfigurations can cause various issues, they don't typically manifest as false concurrent session warnings.

Option C is incorrect. An outage in the collaboration tool would not typically cause a false warning of multiple active sessions.

Question 449. A company is looking for a cryptographic solution that provides an immutable and transparent record of all transactions in a distributed ledger system. Which of the following would BEST meet this requirement?

- (A) Symmetric key algorithm
- (B) Public key infrastructure
- (C) **Blockchain**
- (D) Digital watermark

Explanation 449. Correct Answer: C. Blockchain.

Blockchain is a decentralized and distributed ledger technology that provides an immutable record of transactions. Each block contains a list of transactions and is linked to the previous block, creating a chain. The transparency and immutability of blockchain make it especially suitable for applications where an irrefutable record is essential.

Option A is incorrect. Symmetric key algorithms are encryption methods where the same key is used for both

encryption and decryption but don't inherently provide an immutable record of transactions.

Option B is incorrect. Public key infrastructure (PKI) is used for digital certificates and keys distribution but doesn't offer an immutable record of transactions.

Option D is incorrect. Digital watermarking embeds information into a digital signal, but it doesn't provide an immutable record of transactions.

Question 450. TechCorp is collaborating with SoftTech, a business partner. To streamline collaboration without managing multiple accounts, TechCorp wants its employees to use their existing credentials to access SoftTech's online project management system. Which of the following approaches would BEST enable this functionality?

- (A) TechCorp should create new accounts for its employees on SoftTech's system
- (B) SoftTech should allow anonymous access for TechCorp's employees
- (C) **TechCorp should implement federation between its identity provider and SoftTech's service provider**
- (D) SoftTech should reset all passwords and provide them to TechCorp's employees

Explanation 450. Correct Answer: C. TechCorp should implement federation between its identity provider and SoftTech's service provider. Federation allows two organizations to trust each other's identity systems. TechCorp's

employees can use their existing credentials to access services on SoftTech's system without the need to create new accounts.

Option A is incorrect. Creating new accounts for every user in a collaborating organization isn't scalable and negates the advantages of federation.

Option B is incorrect. Allowing anonymous access would compromise security and wouldn't guarantee identity verification.

Option D is incorrect. Resetting all passwords and providing them anew is not a practical or secure approach to collaboration between two organizations.

Question 451. GlobalTech is implementing a disaster recovery plan and wants to ensure continuous availability with no data loss. They have decided to use replication as a backup strategy. Which of the following replication techniques should GlobalTech implement to achieve their objective?

- (A) Periodic replication scheduled daily
- (B) Asynchronous replication with hourly synchronization
- (C) **Synchronous replication**
- (D) Snapshot replication every 30 minutes

Explanation 451. Correct Answer: C. Synchronous replication. Synchronous replication ensures that data is written to the primary and secondary locations simultaneously, ensuring no data loss and continuous availability. This method is suitable for GlobalTech's requirement of no data loss.

Option A is incorrect. Periodic replication scheduled daily could result in up to a day's worth of data loss in the event of a disaster.

Option B is incorrect. Asynchronous replication with hourly synchronization could lead to an hour's worth of data loss if an incident occurs just before synchronization.

Option D is incorrect. Snapshot replication every 30 minutes could result in 30 minutes of data loss in the event of an incident.

Question 452. An e-commerce website suddenly experiences a sharp increase in traffic, causing the website to become slow and occasionally inaccessible. The IT team observes that a large number of requests are originating from multiple IP addresses spread across various countries. What type of network attack is the e-commerce website likely experiencing?

- (A) Man-in-the-middle attack
- (B) DNS spoofing
- (C) **Distributed denial-of-service (DDoS) attack**
- (D) ARP poisoning

Explanation 452. Correct Answer: C. Distributed denial-of-service (DDoS) attack. In a DDoS attack, the attacker uses multiple systems, often compromised ones from different locations, to flood a target system with requests, making the target slow or inaccessible.

Option A is incorrect. A man-in-the-middle attack involves an attacker secretly intercepting and possibly altering the

communication between two parties. It doesn't lead to website inaccessibility due to high traffic.

Option B is incorrect. DNS spoofing is when an attacker introduces corrupt DNS cache information to redirect traffic to a different IP address, usually under the attacker's control. It doesn't cause increased traffic from various countries.

Option D is incorrect. ARP poisoning is a technique by which an attacker sends fake ARP messages onto a local area network. This is usually used to link an attacker's MAC address with the IP address of another host, causing any traffic meant for that IP address to be sent to the attacker instead.

Question 453. A software development company is working on a mobile banking application. They want to ensure that sensitive operations like cryptographic processes and biometric data validation are isolated from the main operating system to prevent potential tampering. Which tool should they consider implementing to achieve this objective?

- (A) Hardware Security Module (HSM)
- (B) Key Management System (KMS)
- (C) **Secure enclave**
- (D) Trusted Platform Module (TPM)

Explanation 453. Correct Answer: C. Secure enclave. A secure enclave is a hardware-based isolated environment often found in modern CPUs, especially in mobile devices. It's designed to run specific operations such as cryptographic processes and biometric data validation, ensuring that this data

is kept isolated from the main operating system, making it resilient to tampering.

Option A is incorrect. While an HSM is a dedicated hardware device that manages cryptographic keys, it doesn't provide the isolated environment within a CPU for operations like the secure enclave does.

Option B is incorrect. KMS is primarily focused on the management of cryptographic keys, not on creating isolated environments for operations.

Option D is incorrect. TPM provides hardware-level security for individual devices, but it doesn't create a segregated environment within the CPU for operations like the secure enclave.

Question 454. A popular social media platform allows third-party applications to access user data and post on behalf of users. To avoid sharing user passwords with third-party applications and provide limited, scoped access, which authentication method should the platform use?

- (A) Embed user passwords in the application's code
- (B) Use basic authentication with username and password for every request
- (C) **Implement Single Sign-On (SSO) using OAuth to provide token-based access**
- (D) Rely solely on CAPTCHA for third-party app authentication

Explanation 454. Correct Answer: C. Implement Single Sign-On (SSO) using OAuth to provide token-based access.

OAuth provides token-based access and lets third-party applications operate on behalf of users without exposing user passwords. OAuth tokens can also be scoped to limit the range of actions a third-party application can perform.

Option A is incorrect. Embedding passwords in application code is insecure and goes against best practices.

Option B is incorrect. Basic authentication exposes user credentials and doesn't offer the scoped access OAuth provides.

Option D is incorrect. CAPTCHA is designed to differentiate between human and automated access but doesn't handle authentication or authorization.

Question 455. A company has noticed an increase in malware infections over the past month. After investigating, it was determined that the infections were caused by employees visiting websites that were newly registered but had malicious intent. Which of the following would be the BEST approach to mitigate this threat?

- (A) Implement a block rule to deny access to all websites
- (B) Use a web filter that incorporates domain reputation checks and blocks domains registered recently**
- (C) Set the web filter to block all websites not categorized as "Business"
- (D) Enforce multi-factor authentication for all internet-based applications

Explanation 455. Correct Answer: B. Use a web filter that incorporates domain reputation checks and blocks domains registered recently. Reputation-based web filters can evaluate the trustworthiness of domains. One common heuristic is to be suspicious of newly registered domains, as cybercriminals often use these for phishing or malware distribution.

Option A is incorrect. Blocking access to all websites is an extreme measure that would hinder business operations and employee productivity.

Option C is incorrect. Simply blocking websites not categorized as “Business” does not specifically target the threat of newly registered malicious domains. Additionally, some business-relevant websites might not be categorized properly.

Option D is incorrect. While multi-factor authentication can enhance security, it does not address the threat of employees visiting malicious websites.

.Question 456. MetroTech recently experienced an incident where an employee mistakenly deleted a portion of their database. The IT team was able to restore the data using a backup snapshot taken 24 hours prior. However, some data loss still occurred. Which of the following recommendations would minimize data loss in a similar situation in the future?

- (A) Configure backup snapshots to be taken on a weekly basis
- (B) Employ a differential backup solution in addition to snapshots

- (C) Increase the storage capacity for backups
- (D) **Use an hourly snapshot backup schedule**

Explanation 456. Correct Answer: D. Use an hourly snapshot backup schedule. Increasing the frequency of snapshot backups, such as taking them every hour, will ensure that the maximum amount of data that can be lost is limited to that hour's worth. This minimizes the potential for data loss compared to a 24-hour window.

Option A is incorrect. Taking weekly snapshots would actually increase the potential data loss window, not decrease it.

Option B is incorrect. While differential backups capture data changes since the last full backup, they don't necessarily reduce the time window for potential data loss like increasing snapshot frequency would.

Option C is incorrect. Increasing storage capacity allows for more backups or longer retention but does not in itself reduce the time window for potential data loss.

Question 457. Alice receives an email from Bob with an attached document. She wants to verify both the authenticity of the sender and the integrity of the attached document. Which of the following should Bob have used before sending the email?

- (A) Encrypt the document with his private key
- (B) Hash the document
- (C) Encrypt the document with Alice's public key
- (D) **Sign the document with his private key**

Explanation 457. Correct Answer: D. Sign the document with his private key.

Digital signatures are created by taking a hash of a message (or document) and then encrypting that hash with the sender's private key. When Alice receives the email, she can decrypt the signature using Bob's public key to retrieve the original hash and then compare it with her computed hash of the document. If they match, it confirms both the sender's identity (authenticity) and that the document has not been altered (integrity).

Option A is incorrect. Encrypting the entire document with his private key isn't practical for verifying authenticity and integrity. Instead, the hash of the document is encrypted to create a signature.

Option B is incorrect. Simply hashing the document will provide a way to check the document's integrity but does not verify the authenticity of the sender.

Option C is incorrect. Encrypting the document with Alice's public key would make it confidential for Alice, but this doesn't help in verifying authenticity or integrity.

Question 458. An international company, GlobalTech, is using several web applications hosted by different vendors. To ensure their employees can access these applications without having to remember multiple sets of credentials, they want to implement a solution that can securely exchange user authentication information between the company and the service providers. What should GlobalTech implement?

(A) Integrate each application with an independent LDAP

server

(B) Implement SSO using Security Assertions Markup Language (SAML)

(C) Embed encrypted user credentials within the URL of each application

(D) Rely on public API keys shared between the company and each vendor

Explanation 458. Correct Answer: B. Implement SSO using Security Assertions Markup Language (SAML). SAML is an XML-based standard for exchanging authentication and authorization data between parties. It's designed to facilitate single sign-on for web applications. By implementing SSO with SAML, GlobalTech can allow its employees to authenticate once and gain access to multiple applications without re-authenticating.

Option A is incorrect. Having independent LDAP servers for each application defeats the purpose of SSO and complicates user management.

Option C is incorrect. Embedding encrypted user credentials in URLs is insecure and not a recommended practice.

Option D is incorrect. API keys are used for system-to-system communication and not for user authentication. Moreover, public API keys shouldn't be shared recklessly.

Question 459. A user wants to send a confidential email to their colleague and ensure that only the intended recipient can read it. The user also wants to provide assurance to the recipient that

the email was indeed sent by them. Which encryption method should the user employ to accomplish this?

- (A) Use symmetric encryption with a shared key
- (B) Use asymmetric encryption and encrypt the email with the recipient's public key
- (C) Use asymmetric encryption, encrypt the email with the user's private key
- (D) **Use asymmetric encryption, first sign the email with the user's private key, then encrypt it with the recipient's public key**

Explanation 459. Correct Answer: D. Use asymmetric encryption, first sign the email with the user's private key, then encrypt it with the recipient's public key.

Option D offers both confidentiality and non-repudiation.

The email is encrypted with the recipient's public key, ensuring only the recipient can decrypt it using their private key. Signing the email with the sender's private key allows the recipient to verify the sender using the sender's public key.

Option A is incorrect. While symmetric encryption provides confidentiality, it doesn't offer non-repudiation or sender verification.

Option B is incorrect. Encrypting with the recipient's public key provides confidentiality but lacks sender verification.

Option C is incorrect. Encrypting an email with the user's private key would offer sender verification but won't provide confidentiality.

Question 460. DigitalFront, an e-commerce company, is expecting a surge in traffic during their upcoming annual sale event. They want to ensure that their website and applications can handle the anticipated increase in user activity without any performance degradation. Which of the following steps is MOST relevant to achieving this goal?

- (A) Increasing the frequency of security audits
- (B) **Implementing capacity planning specifically focused on technology**
- (C) Adopting multi-factor authentication for all users
- (D) Investing in advanced threat intelligence solutions

Explanation 460. Correct Answer: B. Implementing capacity planning specifically focused on technology.

Capacity planning with a focus on technology ensures that all technological resources, such as servers, bandwidth, storage, and software, are adequately prepared to handle the expected increase in load or traffic, ensuring smooth performance during peak periods.

Option A is incorrect. Security audits are important for identifying vulnerabilities, but they don't address the direct need for scaling technology resources to manage increased traffic.

Option C is incorrect. Multi-factor authentication improves security for users but does not aid in handling a surge in website traffic or user activity.

Option D is incorrect. Advanced threat intelligence solutions provide insights into potential threats, but they don't address technology scaling to accommodate increased traffic.

Question 461. Sarah, a security analyst, is concerned about potential man-in-the-middle attacks on the company's internal portal. To mitigate this risk, she recommends obtaining a digital certificate from a trusted entity. Which of the following is responsible for issuing such certificates?

- (A) Key distribution center
- (B) **Certificate authority (CA)**
- (C) Tokenization system
- (D) Security incident event manager

Explanation 461. Correct Answer: B. Certificate authority (CA). Certificate authorities (CAs) are trusted entities responsible for issuing, validating, and revoking digital certificates. These certificates are used to authenticate entities on the internet, such as websites, ensuring secure and authenticated communications, thus mitigating the risk of man-in-the-middle attacks.

Option A is incorrect. A Key distribution center (KDC) is a part of the Kerberos authentication protocol and is responsible for distributing session tickets and temporary session keys, not for issuing digital certificates.

Option C is incorrect. Tokenization systems replace sensitive data with non-sensitive substitutes, known as tokens. They don't issue digital certificates.

Option D is incorrect. A Security incident event manager (SIEM) aggregates and analyzes log data from various sources, providing real-time analysis of security alerts, but does not issue certificates.

Question 462. A security analyst discovers that an external IP address has been repeatedly trying every possible combination of characters to gain access to the company's VPN portal for the past two days. Which type of password attack is this MOST likely describing?

- (A) Password Spraying
- (B) Dictionary Attack
- (C) Rainbow Table Attack
- (D) **Brute Force Attack**

Explanation 462. Correct Answer: D. Brute Force Attack. A Brute Force Attack involves systematically trying every possible combination of characters until the correct one is found. The scenario specifies that every possible combination of characters is being tried on the VPN portal, indicating a brute force attack.

Option A is incorrect. Password Spraying involves trying a few commonly used passwords across multiple accounts, rather than all possible combinations on one account.

Option B is incorrect. A Dictionary Attack uses a list of common or previously used passwords to attempt access. It doesn't involve trying every possible combination.

Option C is incorrect. A Rainbow Table Attack uses precomputed tables for reversing cryptographic hash functions. This scenario doesn't mention hash values or the use of such tables.

Question 463. A graphic design company frequently works with large files such as videos and high-resolution images. These files are stored on a dedicated storage volume in their server. While they need to secure this data, they don't want to encrypt individual files due to the volume of data and frequent access needs. Which encryption approach is most appropriate for this scenario?

- (A) File-level Encryption
- (B) Full-disk Encryption
- (C) Transport-layer Encryption
- (D) **Volume-level Encryption**

Explanation 463. Correct Answer: D. Volume-level Encryption. Volume-level Encryption allows the encryption of a specific volume or logical drive. In this case, it would allow the company to encrypt the entire volume where these large files are stored without having to encrypt individual files. This ensures the entire volume's contents are encrypted while providing seamless access when required.

Option A is incorrect. File-level Encryption, while effective, would be tedious for encrypting numerous large files individually.

Option B is incorrect. Full-disk Encryption would encrypt the entire disk, which may not be necessary if only a specific volume requires encryption.

Option C is incorrect. Transport-layer Encryption pertains to data in transit and doesn't address the need of encrypting stored data at the volume level.

Question 464. Sarah is a project manager and is working on a document that she owns. She wants to grant specific permissions to certain team members, allowing some to edit and others only to view the document. Which of the following access control models would BEST allow Sarah to accomplish this?

- (A) Mandatory Access Control (MAC)
- (B) Role-Based Access Control (RBAC)
- (C) **Discretionary Access Control (DAC)**
- (D) Attribute-Based Access Control (ABAC)

Explanation 464. Correct Answer: C. Discretionary Access Control (DAC). DAC allows the owner of the resource (in this case, Sarah) to specify who can access it and what permissions they have (e.g., read, write, execute). This flexibility is what Sarah needs to grant specific permissions to individual team members based on her discretion.

Option A is incorrect. Mandatory Access Control (MAC) is based on classifications and clearance levels. It wouldn't be suitable for Sarah's needs in this scenario.

Option B is incorrect. Role-Based Access Control (RBAC) assigns permissions based on roles in the organization. It wouldn't allow Sarah the fine-grained control she needs over individual permissions.

Option D is incorrect. Attribute-Based Access Control (ABAC) bases access on attributes of the user, environment, and resource itself. While flexible, it's not centered around the owner's discretion in the same way DAC is.

Question 465. MegaCorp is transitioning to a cloud-based infrastructure and wants to allow its employees to access multiple cloud services without re-entering their credentials every time. They currently have an on-premises LDAP directory in place. Which approach should MegaCorp take to provide a seamless authentication experience?

(A) MegaCorp should abandon their LDAP directory and create individual accounts for each cloud service

(B) **Integrate their LDAP with a Single Sign-On (SSO) solution that supports cloud services**

(C) Store passwords in a plaintext file for users to access and login to cloud services manually

(D) Force users to change passwords every day to enhance security across all cloud platforms

Explanation 465. Correct Answer: B. Integrate their LDAP with a Single Sign-On (SSO) solution that supports cloud services. By integrating the on-premises LDAP with an SSO solution, MegaCorp can leverage its existing user directory to authenticate and provide access to multiple cloud services without requiring users to log in separately for each service.

Option A is incorrect. Abandoning the existing LDAP directory would negate the benefits of central management and create administrative overhead.

Option C is incorrect. Storing passwords in plaintext is a significant security risk and goes against best practices.

Option D is incorrect. Forcing users to change passwords daily is impractical, could result in weaker passwords, and doesn't provide a seamless authentication experience.

Question 466. A global manufacturing company wants to ensure its employees worldwide do not access websites promoting hate speech, gambling, or explicit content during working hours. To meet this requirement, which web filtering technique would be the most efficient?

- (A) Deploy a centralized proxy with location-based filtering
- (B) Use a blacklist of specific URLs known to contain such content
- (C) **Implement content categorization and block undesired categories**
- (D) Monitor internet usage logs and reprimand violators

Explanation 466. Correct Answer: C. Implement content categorization and block undesired categories. Content categorization is a technique where websites are categorized based on their content type, such as “gaming,” “social media,” “news,” etc. By using this technique, organizations can block entire categories of content, such as “hate speech” or “gambling,” ensuring broad coverage without the need to identify every problematic URL individually.

Option A is incorrect. While centralized proxies can help manage internet access, location-based filtering focuses more on geographic locations rather than content categories.

Option B is incorrect. Relying solely on a blacklist can be inefficient, as it requires constant updates to catch every possible harmful URL, and it might not cover newly created sites quickly enough.

Option D is incorrect. Simply monitoring internet usage logs and reprimanding violators is reactive and does not proactively prevent access to undesired content.

Question 467. During an IT audit, a company's encryption practices come under scrutiny. The IT auditor recommends increasing the encryption key length for certain applications to improve security. What is the PRIMARY reason to increase the encryption key length?

- (A) To speed up encryption and decryption processes
- (B) To ensure compatibility with older systems
- (C) **To reduce the possibility of a brute force attack**
- (D) To reduce the key management overhead

Explanation 467. Correct Answer: C. To reduce the possibility of a brute force attack. Increasing the encryption key length primarily enhances the security of the encryption by making it more resistant to brute-force attacks. A brute force attack involves trying all possible key combinations, and a longer key length means exponentially more possible combinations, making the attack vastly more time-consuming and difficult.

Option A is incorrect. Longer key lengths generally slow down the encryption and decryption processes, as more computational power is required.

Option B is incorrect. Increasing key length might make the encryption incompatible with older systems that do not support the newer, longer key lengths.

Option D is incorrect. Key management overhead typically increases with longer key lengths, as more data must be managed and kept secure.

Question 468. PharmaCorp, a pharmaceutical company, wants to ensure that its researchers cannot transfer proprietary formulas and research data to external storage devices or cloud storage. The company needs a solution to prevent such transfers while allowing other types of data to be transferred. What should they implement?

- (A) Web Application Firewall (WAF)
- (B) Data Encryption Tool
- (C) **Data Loss Prevention (DLP)**
- (D) Virtual Private Network (VPN)

Explanation 468. Correct Answer: C. Data Loss Prevention (DLP). Data Loss Prevention (DLP) is designed to detect potential data breach attempts and prevent the unauthorized transfer of sensitive data. By setting up rules and criteria in a DLP solution, PharmaCorp can restrict the transfer of proprietary information while allowing other data to be transferred as needed.

Option A is incorrect. A Web Application Firewall (WAF) is used to protect web applications by filtering and monitoring HTTP traffic. It does not handle data transfers to external storage or cloud storage specifically.

Option B is incorrect. A Data Encryption Tool encrypts data to protect it from unauthorized access. While it adds a layer of security, it doesn't prevent the transfer of data to external devices or cloud storage.

Option D is incorrect. A Virtual Private Network (VPN) provides a secure tunnel for data transmission between two endpoints. It does not prevent or monitor the type of data being transferred.

Question 469. An online banking platform wants to improve its customer verification process when users open a new account. Which of the following identity proofing methods would be the MOST secure for this purpose?

- (A) Asking users to select a security question and answer from a list
- (B) Requiring users to upload a photo of a government-issued ID and a selfie**
- (C) Sending a verification code to the user's email address
- (D) Prompting users to provide their favorite color

Explanation 469. Correct Answer: B. Requiring users to upload a photo of a government-issued ID and a selfie. This method provides a high level of assurance by comparing a user's live image (selfie) with a government-issued ID. The combination ensures the person is who they claim to be.

Option A is incorrect. Security questions, especially from a pre-defined list, can be easily guessed or obtained by attackers.

Option C is incorrect. Verification codes via email can enhance identity proofing but aren't as robust as checking against a government ID and selfie.

Option D is incorrect. Personal preferences, like favorite colors, are weak indicators of identity and can be easily guessed.

Question 470. Sarah is working on a project where she needs to validate the integrity and authenticity of assets over time, without a centralized authority. Which technology would be most appropriate for this use case?

- (A) Digital signature
- (B) Key escrow
- (C) **Blockchain**
- (D) Key management system

Explanation 470. Correct Answer: C. Blockchain.

Blockchain technology allows for the validation of the integrity and authenticity of assets over time in a decentralized manner. Each transaction or asset is verified by the network's participants and added to the chain, ensuring its authenticity and making it tamper-evident.

Option A is incorrect. While digital signatures can validate the authenticity and integrity of a message or document, they do not provide a decentralized ledger of assets over time.

Option B is incorrect. Key escrow is a method where cryptographic keys are held in trust so that a third party can have access under certain conditions. It doesn't help in validating the integrity and authenticity of assets over time without central authority.

Option D is incorrect. A key management system manages the life cycle of cryptographic keys but does not inherently validate the integrity and authenticity of assets over time.

Question 471. After a recent cyber attack on a corporation's central database, the IT department has been tasked with enhancing the security of their network infrastructure. Which of the following would be the BEST technique to ensure that different departments, like HR and Finance, cannot access each other's sensitive data?

- (A) **Implement network segmentation based on departments**
- (B) Upgrade the bandwidth of the entire network
- (C) Use a single strong password for all departments
- (D) Move all department data to the cloud

Explanation 471. Correct Answer: A. Implement network segmentation based on departments. Network segmentation divides a network into multiple segments or subnets, each acting as its own small network. This limits access between segments and can protect sensitive data by ensuring that only those within a segment can access its resources.

Option B is incorrect. While upgrading the bandwidth may improve network speeds, it does not address the security concern of segregating departmental data.

Option C is incorrect. Using a single strong password for all departments does not prevent one department from accessing another's data. It also introduces a single point of failure.

Option D is incorrect. Moving data to the cloud can offer some security benefits, but without proper access controls and segmentation, different departments could still access each other's data.

Question 472. A finance department employee, Maya, is transferred to the HR department. The IT department is considering her access requirements. Which of the following actions aligns best with the principle of least privilege?

- (A) Retain Maya's access to the finance system and grant additional access to the HR system
- (B) Remove all previous access rights and provide her access solely to the HR system**
- (C) Grant Maya administrative rights to ease her transition between departments
- (D) Limit Maya's access to read-only for both finance and HR systems for a transitional period

Explanation 472. Correct Answer: B. Remove all previous access rights and provide her access solely to the HR system.

When an employee transitions from one department to another, their access requirements change. To uphold the principle of least privilege, it's essential to re-evaluate and adjust access

rights. Maya no longer requires access to the finance system and should only have access to the resources necessary for her new role in HR.

Option A is incorrect. Retaining access to the finance system when Maya no longer works in that department is unnecessary and could be a security risk.

Option C is incorrect. Granting administrative rights is excessive and would provide Maya with more access than necessary for her new role.

Option D is incorrect. While read-only access limits potential damage, providing access to both systems is unnecessary if Maya's new role only requires access to the HR system.

Question 473. A financial institution, BankCorp, has recently experienced a surge in phishing attacks targeting its employees. These attacks often involve URLs that look similar to legitimate ones but have slight variations. To reduce the risk of employees accidentally accessing these malicious sites, which measure should BankCorp implement?

- (A) Implement a Domain Name System (DNS) firewall
- (B) Employ URL scanning to identify and block malicious URLs**
- (C) Rely on manual reporting of suspicious URLs by employees
- (D) Use a Virtual Private Network (VPN) to redirect all employee web traffic

Explanation 473. Correct Answer: B. Employ URL scanning to identify and block malicious URLs. URL scanning can identify potentially malicious sites by examining the complete URL and comparing it with known malicious URLs or patterns. This method can block access to URLs that are designed to look similar to legitimate ones.

Option A is incorrect. While a DNS firewall can help block access to malicious domains, URL scanning provides more granular control by examining the full URL, not just the domain.

Option C is incorrect. Relying solely on manual reporting by employees may not be as efficient or effective as an automated URL scanning solution. It would also place undue responsibility on employees to recognize and report every malicious URL.

Option D is incorrect. Using a VPN simply changes the route of the traffic and provides encrypted communication. It does not inherently offer URL scanning or filtering capabilities.

Question 474. The IT team at a manufacturing company is deploying an IoT-based monitoring system for their machinery. They want to ensure that these IoT devices, if compromised, cannot adversely affect their main corporate network. What should they implement to achieve this?

- (A) Install antivirus software on all IoT devices
- (B) Regularly patch and update the IoT device firmware
- (C) **Place the IoT devices on a dedicated VLAN**
- (D) Enable multi-factor authentication for IoT devices

Explanation 474. Correct Answer: C. Place the IoT devices on a dedicated VLAN. Placing the IoT devices on a dedicated VLAN (Virtual Local Area Network) provides network isolation, ensuring that the devices are segregated from the main corporate network. This strategy ensures that if an IoT device is compromised, it doesn't pose a direct threat to the core corporate network systems.

Option A is incorrect. Many IoT devices may not support traditional antivirus software, and even if they do, this doesn't achieve the network isolation desired.

Option B is incorrect. While regularly patching and updating device firmware is crucial for security, it doesn't provide network isolation from the main corporate network.

Option D is incorrect. Enabling multi-factor authentication can enhance the security of devices but doesn't provide the network isolation specified in the scenario.

Question 475. The content filtering logs at a retail company display multiple instances of blocked access to a file download URL ending with “.exe”. The source IP address belongs to a point of sale (POS) terminal. What should be the primary concern for the security team?

- (A) The POS terminal might have outdated software
- (B) There's a possible misconfiguration in the content filtering rules
- (C) **The POS terminal might be compromised and trying to download malicious executables**
- (D) The company's internet speed is too slow

Explanation 475. Correct Answer: C. The POS terminal might be compromised and trying to download malicious executables. POS terminals shouldn't be downloading executable files from the internet, especially without administrative oversight. Multiple attempts to download ".exe" files could indicate that the POS terminal is compromised and that malicious software is attempting to download further payloads.

Option A is incorrect. While outdated software is a security concern, it wouldn't manifest as multiple blocked attempts to download executables.

Option B is incorrect. Misconfigurations in content filtering rules might block legitimate content, but the specific action of a POS terminal trying to download executable files is suspicious regardless of content filtering rules.

Option D is incorrect. The company's internet speed has no relevance to the specific content being blocked by the filtering system

Question 476. A company wants to implement a solution that verifies the software integrity of remote servers before allowing them to connect to the primary network. Which of the following solutions BEST achieves this objective through attestation?

- (A) Host-based firewall
- (B) Whitelisting application
- (C) **Remote attestation**
- (D) VPN tunneling

Explanation 476. Correct Answer: C. Remote attestation.

Remote attestation is a process where a device (like a server) proves to a remote entity (like a network controller) that it is running genuine, unmodified software. It allows for the verification of the software integrity of remote devices before they connect to a primary network.

Option A is incorrect. A host-based firewall is used to control inbound and outbound network traffic to and from a device based on a set of configurable rules. It does not verify the software integrity of the device itself.

Option B is incorrect. A whitelisting application only allows specified software to run on a system. While it can enhance security by ensuring only approved software runs, it does not attest to the state or integrity of the device or its software when connecting to another network.

Option D is incorrect. VPN tunneling encrypts the connection between two points over the internet. While it ensures secure communication, it doesn't verify the software integrity of devices.

Question 477. ABC Tech has a mixed environment with both Linux and Windows servers. They want to ensure that processes running on their Linux servers only have access to specific resources and are restricted from performing certain actions. Which of the following tools would be most appropriate for this task?

(A) Use Group Policy on their Windows servers and apply it to Linux servers

- (B) Implement a strict user training regimen to inform users about security best practices
- (C) **Enable Security-Enhanced Linux (SELinux) in enforcing mode**
- (D) Limit user access to Linux servers

Explanation 477. Correct Answer: C. Enable Security-Enhanced Linux (SELinux) in enforcing mode. SELinux provides mandatory access controls by limiting the actions a process can perform to only those defined in its policy, ensuring it only has access to specific resources. By setting SELinux in enforcing mode, these policies are actively enforced.

Option A is incorrect. Group Policy is specific to Windows and cannot be applied directly to Linux servers.

Option B is incorrect. While user training is a good security practice, it does not provide the technical control required to restrict processes on Linux servers.

Option D is incorrect. Limiting user access to Linux servers does not directly control the actions of processes running on those servers.

Question 478. Liam, a security analyst, is investigating a potential breach. He discovers that a malicious actor sent requests to the server by altering HTTP headers to impersonate another user, thereby gaining unauthorized access. Which type of application attack is this?

- (A) Cross-Site Request Forgery (CSRF)
- (B) Cross-Site Scripting (XSS)

- (C) HTTP Header Forgery
- (D) Session Hijacking

Explanation 478. Correct Answer: C. HTTP Header Forgery. HTTP Header Forgery involves manipulating HTTP headers in a request to impersonate, spoof, or deceive systems, often for bypassing security controls or impersonating other users. In the described scenario, the malicious actor altered HTTP headers to impersonate another user, indicating an HTTP Header Forgery attack.

Option A is incorrect. Cross-Site Request Forgery (CSRF) involves tricking a user into executing actions on a web application where they're authenticated, without their knowledge. While it involves forgery, it doesn't involve directly manipulating HTTP headers as described.

Option B is incorrect. Cross-Site Scripting (XSS) involves injecting malicious scripts into web content viewed by other users. The scenario does not pertain to injecting scripts.

Option D is incorrect. Session Hijacking involves taking over a user's session to perform unauthorized actions. It doesn't specifically involve the manipulation of HTTP headers.

Question 479. ABC Corp has recently faced a security breach due to a contractor connecting an infected laptop to the corporate network. Management wants to implement a solution that would ensure that any device connecting to the corporate network meets the company's security standards, including up-to-date antivirus definitions. Which solution should ABC Corp

consider?

- (A) Intrusion Detection System (IDS)
- (B) Virtual Private Network (VPN)
- (C) **Network Access Control (NAC)**
- (D) Web Application Firewall (WAF)

Explanation 479. Correct Answer: C. Network Access Control (NAC). Network Access Control (NAC) allows organizations to set policies for device connectivity to corporate networks. NAC can assess the security posture of a device before it connects to ensure it meets predefined criteria, such as updated antivirus definitions, required patches, etc.

Option A is incorrect. An Intrusion Detection System (IDS) monitors network traffic for suspicious activities and issues alerts but does not evaluate device security postures before allowing network access.

Option B is incorrect. A Virtual Private Network (VPN) allows secure remote access to a network but does not inherently evaluate the security posture of devices.

Option D is incorrect. A Web Application Firewall (WAF) focuses on protecting web applications by monitoring and filtering HTTP traffic. It is not used for evaluating device security postures.

Question 480. CyberFirm has been facing issues with phishing campaigns where attackers spoof their domain to send fraudulent emails. They already implemented DKIM to sign their emails but want an additional measure to specify which

mail servers are authorized to send emails on behalf of their domain. Which security measure should CyberFirm adopt?

- (A) SPF
- (B) PGP
- (C) SSL certificate
- (D) IMAP

Explanation 480. Correct Answer: A. SPF. Sender Policy Framework (SPF) is designed to prevent email spoofing. It allows domain owners to specify which mail servers are authorized to send emails on behalf of their domain. Receiving servers can then verify the sending server against the SPF record in the domain's DNS.

Option B is incorrect. PGP (Pretty Good Privacy) is used for encrypting and decrypting texts, emails, files, directories, and whole disk partitions, but it doesn't define authorized mail servers for a domain.

Option C is incorrect. An SSL certificate provides a secure connection between a user's web browser and a website, ensuring data confidentiality. It's not specifically designed to validate the sending mail servers of a domain.

Option D is incorrect. IMAP (Internet Message Access Protocol) is a protocol used by email clients to retrieve messages from a mail server. It doesn't help in specifying authorized mail servers for a domain.

Question 481. A web application requires users to authenticate using a token sent to their email. Alex, a security analyst,

observes that once logged in, if he presents the same token again, he is granted access without any restrictions. What type of vulnerability does this situation depict?

- (A) Cross-Site Request Forgery (CSRF)
- (B) **Replay Attack**
- (C) Man-in-the-Middle (MitM) Attack
- (D) Cross-Site Scripting (XSS)

Explanation 481. Correct Answer: B. Replay Attack. A replay attack, also known as playback attack, occurs when an attacker intercepts data and then retransmits it. In this scenario, Alex was able to reuse the authentication token to gain access, indicating that the system does not have mechanisms in place to prevent replayed tokens from being accepted multiple times.

Option A is incorrect. Cross-Site Request Forgery (CSRF) is an attack where an attacker tricks the victim into performing unwanted actions on a web application where they're authenticated. It doesn't involve reusing authentication tokens.

Option C is incorrect. While a Man-in-the-Middle (MitM) Attack can involve intercepting data between two parties, the described scenario doesn't involve an attacker modifying or relaying the information in real-time.

Option D is incorrect. Cross-Site Scripting (XSS) vulnerabilities allow attackers to inject malicious scripts into web pages. The scenario doesn't indicate any script injection

Question 482. A large law firm has a centralized document repository where lawyers store client information, legal drafts,

and other sensitive data. A new paralegal, Jenna, joins the firm and needs to be able to view client documents but should not be able to modify or delete them. Which type of permission should be granted to Jenna?

- (A) Read-Only
- (B) Full Control
- (C) Modify
- (D) Execute

Explanation 482. Correct Answer: A. Read-Only. The Read-Only permission allows users to view and open files or resources but does not allow them to modify, delete, or execute them. In this scenario, granting Jenna Read-Only access ensures she can view client documents without making any alterations or deletions.

Option B is incorrect. Full Control would give Jenna the ability to modify, delete, and even change the permissions of the documents, which exceeds the necessary permissions for her role.

Option C is incorrect. The Modify permission allows a user to make changes to documents, which is not appropriate for Jenna based on the scenario's requirements.

Option D is incorrect. Execute permission is typically related to running programs or scripts and is not relevant to Jenna's need to view documents.

Question 483. The IT department of a software development company wants to ensure that only company-approved

development tools can be executed in their development environment, preventing any unauthorized or potentially harmful software from running. What should the IT department employ to achieve this?

- (A) Implement network segmentation
- (B) Conduct regular vulnerability assessments
- (C) Install a stateful firewall
- (D) **Establish an application allow list**

Explanation 483. Correct Answer: D. Establish an application allow list. Establishing an application allow list would ensure that only specific, pre-approved applications can run in the development environment. This would prevent any unauthorized or potentially malicious software from being executed, aligning directly with the company's goal.

Option A is incorrect. While network segmentation can isolate different parts of the network and limit the spread of potential threats, it does not prevent unauthorized applications from running within a segment.

Option B is incorrect. Regular vulnerability assessments identify weaknesses in systems, but they don't proactively prevent specific applications from running.

Option C is incorrect. A stateful firewall monitors the state of active connections and can block or allow traffic based on stateful parameters, but it doesn't regulate which applications can be executed on a workstation.

Question 484. A company is implementing a system to ensure that code released to production is both unaltered and approved by a specific team member. Which of the following cryptographic techniques should they implement?

- (A) Symmetric encryption of the code
- (B) Hashing the code with SHA-256
- (C) Encrypting the code with the team member's public key
- (D) **Digital signature by the team member**

Explanation 484. Correct Answer: D. Digital signature by the team member. Digital signatures provide both integrity and non-repudiation. By having the specific team member digitally sign the code, the company can ensure that the code has not been altered (integrity) and that it was approved by the designated individual (non-repudiation).

Option A is incorrect. Symmetric encryption provides confidentiality, but it doesn't provide the needed integrity and non-repudiation in this scenario.

Option B is incorrect. Hashing the code provides a mechanism to check for alterations (integrity), but it does not provide non-repudiation or evidence of the specific team member's approval.

Option C is incorrect. Encrypting with the team member's public key doesn't provide non-repudiation. Moreover, only the team member with the corresponding private key would be able to decrypt it, which might not be desirable for production releases.

Question 485. During an organization's security review, the cybersecurity analyst noticed that there were multiple failed login attempts for different user accounts, each with a few commonly used passwords. What type of password attack does this scenario BEST describe?

- (A) Brute Force Attack
- (B) Dictionary Attack
- (C) Credential Stuffing
- (D) **Password Spraying**

Explanation 485. Correct Answer: D. Password Spraying.

Password Spraying is an attack method where the attacker tries a few commonly used passwords against multiple user accounts, rather than trying many passwords against a single account. The scenario described shows multiple user accounts with common passwords being targeted, aligning with this method.

Option A is incorrect. A Brute Force Attack involves trying all possible password combinations for a particular account. The scenario describes trying common passwords on multiple accounts, not exhaustive combinations on one.

Option B is incorrect. A Dictionary Attack involves trying a list of probable passwords, often extracted from dictionaries or common password lists, against a single account. The scenario emphasizes multiple accounts.

Option C is incorrect. Credential Stuffing involves using previously leaked username and password pairs to gain unauthorized access. The emphasis is on using known credentials, not common passwords.

Question 486. A project manager is working on a new product launch and has documents with sensitive financial projections on her local computer. She occasionally shares these documents with select board members via email. While she wants to keep the financial documents secure, she doesn't want to encrypt all the data on her computer. Which encryption approach should she utilize?

- (A) Full-disk Encryption
- (B) Transport-layer Encryption
- (C) **File-level Encryption**
- (D) Partition Encryption

Explanation 486. Correct Answer: C. File-level Encryption.

File-level Encryption allows individual files or folders to be encrypted. In this scenario, the project manager can encrypt only the sensitive financial documents, allowing her to securely share them while keeping the rest of her data unencrypted.

Option A is incorrect. Full-disk Encryption would encrypt the entire drive, which is more than what's required.

Option B is incorrect. Transport-layer Encryption protects data in transit, but does not specifically address encrypting individual files for storage and sharing.

Option D is incorrect. Partition Encryption encrypts entire partitions or volumes, which isn't necessary in this scenario.

Question 487. A financial institution is looking to adopt an encryption algorithm for its transactions that is considered to be very secure due to its longer key length, compared to older

standards. Which encryption algorithm best fits this description?

- (A) DES
- (B) Blowfish
- (C) RSA
- (D) AES-256

Explanation 487. Correct Answer: D. AES-256. AES-256, part of the Advanced Encryption Standard (AES) family, utilizes a 256-bit key length. This extended key length provides a higher degree of security and is considered resistant to all known practical attacks when used properly.

Option A is incorrect. DES (Data Encryption Standard) has a key length of only 56 bits and is considered to be insecure against sufficiently equipped attackers due to its shorter key length.

Option B is incorrect. While Blowfish is a symmetric encryption algorithm, it's older and not as universally recommended for secure transactions as AES.

Option C is incorrect. RSA is an asymmetric encryption algorithm, not typically used directly for encrypting bulk transaction data.

Question 488. The IT team of XYZ Corp received an alert that an employee's account was used to access the company's portal from Paris at 2:00 PM and then from Tokyo at 2:30 PM. The employee is currently on a business trip to Paris. What could this alert be indicating?

- (A) The employee quickly traveled from Paris to Tokyo

- (B) The company's time zone settings are misconfigured
- (C) There's a possible VPN misconfiguration on the employee's computer
- (D) **The employee's account might have been compromised**

Explanation 488. Correct Answer: D. The employee's account might have been compromised. Impossible travel, in this context, refers to the improbable nature of someone being in two distant geographical locations within a short time frame. Given the close time proximity of both access attempts, it's highly improbable that the employee traveled from Paris to Tokyo in half an hour. This is a common indicator of account compromise.

Option A is incorrect. It's virtually impossible for someone to travel from Paris to Tokyo in just 30 minutes.

Option B is incorrect. Time zone misconfigurations might cause timestamp discrepancies, but they wouldn't cause the appearance of logins from two distant cities within such a short time frame.

Option C is incorrect. Even if there's a VPN misconfiguration, it would not explain the access from two very different geographical locations in such a short span of time.

Question 489. Global Corp received a report that some of its customers received phishing emails that seemed to originate from the company's domain. The IT team checked and confirmed that SPF and DKIM configurations were correctly

set. What additional email security measure can Global Corp implement to provide clear policies on how the emails should be treated if they don't align with SPF and DKIM?

- (A) Enabling TLS encryption
- (B) **Implementing DMARC policies**
- (C) Setting up a new SMTP server
- (D) Increasing email retention period

Explanation 489. Correct Answer: B. Implementing DMARC policies. By implementing DMARC policies, Global Corp can define how email receivers should handle emails from its domain that don't align with the specified SPF and DKIM records. DMARC can be set to monitor, quarantine, or reject emails that fail these checks, providing more robust protection against email spoofing and phishing.

Option A is incorrect. While TLS encryption is essential for protecting the content of email in transit, it doesn't address the issue of spoofing or provide guidelines on how to handle emails that don't match SPF and DKIM.

Option C is incorrect. Setting up a new SMTP server can help with sending emails, but it doesn't inherently protect against email spoofing or provide guidance for emails that don't align with SPF and DKIM.

Option D is incorrect. Increasing the email retention period affects how long emails are stored but doesn't offer protection against spoofing or guidance for handling misaligned emails.

Question 490. A financial institution plans to provide access to its database for third-party developers to create new applications. However, they want to ensure that the developers do not see the actual data but instead work with a disguised version that retains the data's original structure. What technique is the financial institution considering?

- (A) Tokenization
- (B) **Data masking**
- (C) Encryption
- (D) Digital watermarking

Explanation 490. Correct Answer: B. Data masking. Data masking is a technique that obscures specific data within a database, making the data unreadable and unusable. The method is often employed in non-production environments to protect the data subject's data privacy and data security.

Option A is incorrect. Tokenization replaces sensitive data with random tokens, which act as references to the original data.

Option C is incorrect. Encryption converts readable data into an unreadable format to protect its confidentiality. It requires a key to return the data to its original form.

Option D is incorrect. Digital watermarking embeds data into a digital signal, primarily for asserting rights or ownership.

Question 491. While reviewing web server logs, Sarah, a security analyst, notices a pattern of requests containing “..%2F..” in the URLs. She suspects this might be an attempt to exploit a vulnerability. Which type of application attack is likely

being attempted?

- (A) Command Injection
- (B) Cross-Site Scripting (XSS)
- (C) **Directory Traversal**
- (D) Cross-Site Request Forgery (CSRF)

Explanation 491. Correct Answer: C. Directory Traversal.

Directory traversal (also known as path traversal) involves manipulating variables referencing files with “..” sequences and its variations (like “..%2F..”, which URL-decodes to “../..”) to navigate outside of the intended directory. This can allow an attacker to access restricted files on the web server. The pattern Sarah observed in the logs indicates a directory traversal attack attempt.

Option A is incorrect. Command injection attacks involve executing arbitrary commands on the server via application vulnerabilities. The specific pattern observed in the logs does not suggest command execution.

Option B is incorrect. Cross-Site Scripting (XSS) attacks involve injecting malicious scripts into web pages viewed by other users. The pattern observed doesn’t pertain to script injection.

Option D is incorrect. Cross-Site Request Forgery (CSRF) tricks victims into submitting a malicious request. It does not involve directory or path manipulation as described in the scenario.

Question 492. A financial firm outsources its payment processing to a third-party service provider. After a series of fraudulent transactions, it was discovered that the service provider was not employing the latest encryption standards when transmitting data. Which vulnerability related to supply chain does this scenario highlight?

- (A) Inadequate vendor background checks
- (B) **Service provider's outdated security practices**
- (C) Deficient hardware components from a supplier
- (D) Software with embedded backdoors

Explanation 492. Correct Answer: B. Service provider's outdated security practices. Supply chain vulnerabilities encompass risks originating from third-party vendors and service providers. In this scenario, the third-party service provider's failure to use current encryption standards for transmitting data exemplifies a vulnerability that arises due to outdated security practices by the service provider.

Option A is incorrect. While vendor background checks are essential, the scenario does not specifically point towards a problem with the vendor's background. It focuses on their encryption practices.

Option C is incorrect. The scenario doesn't mention hardware components or any issues related to them.

Option D is incorrect. The issue here pertains to encryption standards, not to software with embedded backdoors.

Question 493. A security analyst is evaluating security enhancements for a series of laptops that will store highly confidential data. The analyst wants to ensure that stored data remains encrypted and the integrity of the boot process is maintained. Which of the following would BEST meet this requirement?

- (A) Installing antivirus software on each laptop
- (B) Enabling a software-based full-disk encryption
- (C) Implementing a BIOS password
- (D) Utilizing a Trusted Platform Module (TPM)

Explanation 493. Correct Answer: D. Utilizing a Trusted Platform Module (TPM). A Trusted Platform Module (TPM) is a specialized chip on an endpoint device that stores RSA encryption keys specific to the host system. It provides hardware-based security to enhance the security of the device by enabling features like hardware-based encryption and ensuring the integrity of the boot process, among other things.

Option A is incorrect. While antivirus software is vital for protecting against malware, it does not directly address hardware-based encryption or boot process integrity.

Option B is incorrect. Software-based full-disk encryption can ensure the confidentiality of data, but it does not offer hardware-level protection or boot process integrity like a TPM.

Option C is incorrect. A BIOS password provides a layer of security, but it does not offer encryption for stored data or ensure boot process integrity.

Question 494. An organization is choosing a hash function for digital signatures. They want to ensure that it is resistant to scenarios where an attacker might produce two different messages having the same hash. Which type of attack are they trying to defend against?

- (A) Side-channel Attack
- (B) Replay Attack
- (C) **Birthday Attack**
- (D) Ciphertext-only Attack

Explanation 494. Correct Answer: C. Birthday Attack. In a Birthday Attack, attackers exploit the mathematics behind the birthday problem in probability theory, aiming to find two different inputs that produce the same output, or hash. When selecting a hash function for digital signatures, it's crucial to pick one that is resistant to Birthday Attacks to maintain the integrity of the signatures.

Option A is incorrect. A Side-channel Attack involves obtaining information from the physical implementation of a cryptographic system rather than exploiting a theoretical weakness in algorithms or protocols. It's unrelated to producing two messages with the same hash.

Option B is incorrect. A Replay Attack involves intercepting data (like a login session) and then resending or replaying it to gain unauthorized access. It does not focus on matching hash values.

Option D is incorrect. In a Ciphertext-only Attack, the attacker has the ciphertext and tries to derive the plaintext without

knowing the key. The scenario does not describe this type of attack.

Question 495. At ExamsDigest, employees can access the company's cloud-based storage system. However, access to certain files within the storage is determined by the employee's department, job title, and years of service. For instance, senior managers in the finance department with more than five years of service can view the company's financial forecasts. Which access control model is ExamsDigest using?

- (A) Rule-Based Access Control (RAC)
- (B) Role-Based Access Control (RBAC)
- (C) **Attribute-Based Access Control (ABAC)**
- (D) Discretionary Access Control (DAC)

Explanation 495. Correct Answer: C. Attribute-Based Access Control (ABAC). Attribute-Based Access Control (ABAC) determines access based on attributes of the user, resource, and environment. In the scenario, the employee's department, job title, and years of service are the attributes that determine their access to specific files.

Option A is incorrect. RAC works based on predefined rules, typically without involving multiple user attributes like department or job title.

Option B is incorrect. While RBAC is close in functionality, it assigns permissions based on roles (like "manager" or "clerk"), not on a combination of attributes.

Option D is incorrect. DAC allows resource owners to specify who can access their resources based on their discretion. It doesn't involve a combination of attributes to determine access.

Question 496. After a recent system upgrade, CloudTech Corp. decided to validate the efficiency and reliability of its new data processing system. To do this, they run the new system alongside the old one and compare the outcomes. This way, they aim to ensure that the new system is both robust and capable of handling the current workload. What kind of testing is CloudTech Corp. utilizing?

- (A) Load Testing
- (B) Failover Testing
- (C) **Parallel Processing Testing**
- (D) Simulation Testing

Explanation 496. Correct Answer: C. Parallel Processing Testing. Parallel Processing Testing involves running two systems simultaneously (typically the new one and the old one) to compare the outcomes. This kind of testing ensures that a new system is as effective and reliable as the previous one.

Option A is incorrect. Load Testing checks the system's ability to handle the expected volume of transactions and to see if it can maintain acceptable response times.

Option B is incorrect. Failover Testing is done to ensure that a system can switch to a backup or secondary system in the case of a failure, rather than comparing two systems for consistency.

Option D is incorrect. Simulation Testing involves creating a model of the system under test and stimulating it with virtual users or devices to understand its behavior under various conditions.

Question 497. SecureNet Inc. recently upgraded their security infrastructure. To validate how the new system would respond in real-world scenarios without exposing it to actual risks, they decide to imitate certain cyber threats in a controlled environment. Which type of test is SecureNet Inc. planning to conduct?

- (A) Penetration Testing
- (B) **Simulation Testing**
- (C) Vulnerability Assessment
- (D) Failover Testing.

Explanation 497. Correct Answer: B. Simulation Testing.

Simulation testing involves creating a model of the system under test and then stimulating it with virtual users or devices to understand its behavior under various conditions. In the context of cybersecurity, this means imitating cyber threats in a controlled environment to assess how security infrastructure responds.

Option A is incorrect. Penetration Testing involves ethical hackers attempting to breach an organization's defenses, which involves actual risks, rather than just a simulation.

Option C is incorrect. A Vulnerability Assessment identifies, quantifies, and prioritizes vulnerabilities in a system but doesn't necessarily imitate threats in a controlled environment.

Option D is incorrect. Failover Testing ensures that a system can switch to a backup or secondary system in case of a failure, and does not focus on simulating threats.

Question 498. A marketing team is collaborating on a new campaign and requires access to a shared folder. However, they shouldn't be able to modify files created by others. How should permissions be set on this shared folder?

- (A) Assign the marketing team full control
- (B) Allow the marketing team read-only access
- (C) Assign the marketing team write-only access
- (D) Assign the marketing team modify permission but deny the delete permission**

Explanation 498. Correct Answer: D. Assign the marketing team modify permission but deny the delete permission. By providing modify permissions but denying delete permissions, team members can create and edit their own files, but they won't be able to delete or modify files created by others.

Option A is incorrect. Full control would allow team members to modify or delete any file, which is not desired.

Option B is incorrect. Read-only access would prevent team members from creating or editing any files.

Option C is incorrect. Write-only access would prevent team members from viewing existing files in the folder.

Question 499. An organization's e-commerce platform experienced a data breach where attackers exploited a known

vulnerability. Post-incident analysis revealed that a patch was available for this vulnerability two months before the breach but was not applied. Which of the following would have been the MOST effective measure to prevent this breach?

- (A) Implementing stronger user authentication methods
- (B) Increasing network monitoring for signs of malicious activity
- (C) **Applying the available patch in a timely manner**
- (D) Migrating to a different e-commerce platform

Explanation 499. Correct Answer: C. Applying the available patch in a timely manner. Patches are developed by software vendors to address known vulnerabilities in their software. Timely application of these patches is crucial to ensuring that systems are protected against known threats. In this scenario, applying the available patch would have directly addressed the vulnerability that was exploited.

Option A is incorrect. While implementing stronger user authentication methods can enhance security, it wouldn't directly mitigate a vulnerability in the software that could be exploited without authentication.

Option B is incorrect. Increasing network monitoring can help detect malicious activity, but it doesn't prevent the exploitation of a known software vulnerability.

Option D is incorrect. Migrating to a different platform is a drastic measure that might introduce new vulnerabilities and would not ensure security unless accompanied by good patch management practices.

Question 500. A security analyst is reviewing network logs and notices that an attacker positioned in between the user and the target website is intercepting and potentially modifying the user's communications before passing them on to the intended destination. This malicious activity occurs transparently, with neither the user nor the target website being aware. What type of network attack is being described?

- (A) Replay Attack
- (B) Smurf Attack
- (C) **On-path Attack**
- (D) Spoofing Attack

Explanation 500. Correct Answer: C. On-path Attack. An On-path Attack, also known as a Man-in-the-Middle (MitM) attack, involves an attacker intercepting communications between two parties, potentially modifying the communication, and then relaying it to the intended recipient. Both the source and the destination are unaware of the attacker's presence.

Option A is incorrect. A Replay Attack involves capturing legitimate data packets and retransmitting them at a later time to create an unauthorized effect. It doesn't involve active interception and modification in real-time.

Option B is incorrect. A Smurf Attack is a type of denial-of-service attack that uses ICMP Echo (ping) traffic to flood a target system. It has no relation to intercepting and modifying user communications.

Option D is incorrect. Spoofing Attack involves pretending to be something or someone else. While on-path attacks might

involve some elements of spoofing, the specific action described in the scenario is more aligned with an on-path attack.

EXAM SIMULATOR #6

Questions 501-600

Question 501. A company's website was temporarily defaced with a humorous meme, but no sensitive data was stolen or any significant damage done. The attacker left a message bragging about their first successful hack. Which type of threat actor is MOST likely responsible for this attack?

- (A) Insider threat
- (B) Advanced Persistent Threat (APT)
- (C) Unskilled attacker
- (D) Nation-state

Question 502. A financial institution has experienced an uptick in unauthorized transactions. They want to implement a control that will allow them to identify suspicious transactions in real-time. Which of the following would be the BEST detective control for this scenario?

- (A) Implementing a multi-factor authentication system for all users
- (B) Establishing a Security Operations Center (SOC) to monitor network traffic
- (C) Installing an Intrusion Detection System (IDS) on their network

(D) Restricting transaction capabilities to only a few trusted IP addresses.

Question 503. GammaTech has a new remote access policy for its employees. Whenever an employee attempts to access the corporate network from an unfamiliar location, the system requests additional verification before granting access. Which factor of authentication is being emphasized in this policy?

- (A)** Knowledge-based questions the employee answers
- (B)** A fingerprint scan from the employee
- (C)** The physical coordinates of the employee's access point
- (D)** An SMS code sent to the employee's phone

Question 504. The cybersecurity team of XYZ Corp. plans to assess their organization's preparedness for a potential data breach. They aim to evaluate the effectiveness of their response strategy without performing any real actions. Which of the following methods would BEST help them achieve this goal?

- (A)** Live fire exercise
- (B)** System hardening test
- (C)** Red team/blue team exercise
- (D)** Tabletop exercise

Question 505. A company is attempting to verify the legitimacy of an email sent from a senior executive to a number of employees. The email requests the recipients to click on a link and enter their credentials for a "system upgrade." The security team wants to ascertain if the email genuinely came from the executive. Which of the following metadata from the email would be MOST beneficial in this investigation?

- (A)** The email's subject line

- (B) The email's send time and date
- (C) The originating IP address in the email headers
- (D) The size of the email in bytes

Question 506. An online banking website employs a system that automatically logs out users after 10 minutes of inactivity to ensure that if a user forgets to log out, no one else can alter the user's banking details. Which principle of the CIA triad is the banking website MOST directly addressing?

- (A) Confidentiality
- (B) Availability
- (C) Authentication
- (D) Integrity

Question 507. An IT department in a large corporation spends several hours each day manually deploying patches and updates to thousands of workstations. Which of the following solutions would BEST enhance the efficiency of this process and save time for the IT team?

- (A) Disable automatic updates and conduct monthly patching sessions
- (B) Implement an automated patch management system
- (C) Designate a dedicated team for patching that operates in shifts
- (D) Educate users to install updates on their own

Question 508. Epsilon Inc. recently hired Jenny as a junior network administrator. To ensure security, they give Jenny only the access permissions necessary to complete her specific tasks, such as monitoring network traffic, but not modifying firewall rules. This approach of granting Jenny's permissions aligns with

which security principle?

- (A) Mandatory Access Control (MAC)
- (B) Role-Based Access Control (RBAC)
- (C) Time-of-Day Restrictions
- (D) Least Privilege

Question 509. As part of a cloud infrastructure project, AlphaTech plans to deploy multiple virtualized resources for its new application. The deployment includes databases, web servers, and load balancers. What is the PRIMARY benefit of using automation scripts in the resource provisioning process for this project?

- (A) It enables AlphaTech to use a single operating system for all resources
- (B) It guarantees 100% uptime for all virtualized resources
- (C) It ensures standardized, repeatable, and rapid deployments across the infrastructure
- (D) It prevents unauthorized users from accessing the cloud infrastructure

Question 510. CyberSec Corp's CISO wants to determine if there have been any anomalies in user behavior over the past month. Specifically, they're concerned about unauthorized data transfers outside of regular business hours. Which of the following automated reports would be MOST useful in this investigation?

- (A) After-hours network activity reports
- (B) User password change frequency reports
- (C) Hardware inventory audit reports
- (D) Software licensing compliance reports

Question 511. During a review of IDS logs, a security specialist notices a series of alerts indicating that a single external IP has been sending payloads that exploit a known vulnerability. However, the internal system to which these payloads are sent is patched and is not vulnerable to the exploit. Which of the following describes this type of IDS alert?

- (A) False positive
- (B) False negative
- (C) True positive
- (D) True negative

Question 512. An organization recently experienced a malware infection on one of its workstations. A security analyst has been tasked with reviewing the endpoint logs of the infected system to gather more information about the incident. Which of the following entries in the endpoint logs would be MOST indicative of the initial malware infection point?

- (A) Logs indicating successful user login and logout events
- (B) Entries showing periodic system health-check status as "OK"
- (C) Logs documenting a recently installed and executed unknown .exe file from a temporary directory
- (D) Entries detailing network connectivity checks to the domain controller

Question 513. A security analyst is reviewing the IPS logs and discovers multiple alerts originating from a single IP address attempting to access various company servers. The analyst is trying to determine the type of attack. Which of the following log entries BEST indicates a port scanning activity?

- (A) **Multiple consecutive connection attempts to different**

ports on a single server in a short time frame

- (B) Repeated connection attempts to port 80 of a web server every 3 seconds
- (C) Numerous failed login attempts to an FTP server from the same IP address
- (D) Consistent pings to the network gateway every 5 seconds

Question 514. A global financial company experiences sporadic cyber attacks on its infrastructure. The company notices that attacks that occur during non-business hours often result in more significant damage due to delayed responses. Which of the following measures would BEST decrease the reaction time to these off-hour attacks?

- (A) Train the security staff to handle larger volumes of incidents during business hours
- (B) Implement an automated intrusion detection and response system
- (C) Increase the number of security staff during non-business hours
- (D) Send email notifications to security personnel when attacks are detected

Question 515. GreenTech, a data center company, is planning to expand its operations in a region known for frequent power outages. To maintain security posture and ensure continuity of operations, which of the following should be their PRIMARY consideration regarding power?

- (A) Using power-efficient servers to reduce electricity costs
- (B) Setting up solar panels to promote green energy
- (C) Investing in redundant power supplies and

uninterruptible power systems (UPS)

(D) Running operations only during peak daylight hours to ensure natural lighting

Question 516. A medium-sized enterprise is concerned about the security of its office workstations after a series of malware infections. As a security analyst, which of the following recommendations would BEST improve the security baseline of the workstations?

(A) Install multiple antivirus solutions to ensure maximum detection

(B) Set up screensavers with cyber hygiene tips to educate users

(C) Disable unnecessary services and ports on the workstations

(D) Frequently change the desktop wallpaper to prevent monotony

Question 517. A large financial institution is planning to upgrade its IT infrastructure to allow for a more efficient use of hardware resources, faster deployment of applications, and reduced server provisioning times. While evaluating different technologies, which of the following would directly address these needs?

(A) Network Segmentation

(B) Intrusion Detection System

(C) Virtualization

(D) Multi-Factor Authentication

Question 518. The security team of a multinational company deployed a network of honeypots globally, making it appear as

an interconnected and realistic environment. They aim to study coordinated multi-stage attacks. This deceptive setup is known as:

- (A) Firewall Cluster
- (B) Virtual LAN (VLAN)
- (C) Distributed Denial of Service (DDoS) Prevention
- (D) Honeynet

Question 519. Sophia, the CFO of a medium-sized company, received a call from an individual claiming to be from the IT department. The caller requested her login details for a “critical system update.” Suspecting something wasn’t right, Sophia hung up and contacted her IT department, which confirmed no such call was made by them. Which type of attack did Sophia most likely experience?

- (A) Vishing
- (B) Phishing
- (C) SQL Injection
- (D) Cross-Site Request Forgery (CSRF)

Question 520. Sophia received an email from her bank asking her to urgently update her personal details due to a system upgrade. The email contains a link that redirects to a website that looks similar to her bank’s website. Which of the following should she do FIRST?

- (A) Follow the link and promptly update her personal details to avoid any inconvenience
- (B) Forward the email to her friends and family to ensure they are also aware of the bank's system upgrade
- (C) Delete the email immediately without taking any action

(D) Contact her bank through official channels to verify the authenticity of the email

Question 521. Tech Enterprises is planning to release a new product. As part of the product's creation, they've sourced components from various vendors. The security team is tasked with assessing risks linked to the supply chain. Which of the following is the MOST concerning risk when sourcing components from multiple vendors?

- (A)** Difficulty in tracking product warranty details from multiple vendors
- (B)** Increased product assembly time due to varied vendor delivery timelines
- (C)** Potential for introduction of insecure or compromised components
- (D)** The need for multiple purchase orders, leading to increased paperwork

Question 522. ThetaTech, a financial institution, wants to upgrade its authentication system for high-net-worth customers accessing their accounts online. Besides the traditional password, they want to include a method that captures unique physical or behavioral characteristics. Which type of authentication method should ThetaTech consider?

- (A)** Token-based authentication
- (B)** Geolocation tracking
- (C)** Biometrics
- (D)** Smart card

Question 523. A software development team in a large corporation decided to use an unauthorized cloud-based tool to

host and manage their source code. The team believed it would increase their productivity, even though it was not approved by the IT department. A few weeks later, unauthorized access to their project data was detected. Which threat actor concept BEST describes the situation?

- (A) Insider threat
- (B) Hacktivist
- (C) Shadow IT
- (D) Organized crime syndicate

Question 524. TechHaus has recently experienced multiple security breaches where unauthorized personnel have managed to infiltrate their server rooms after hours. To enhance security measures, the company decided to deploy a new system. Which of the following options would BEST detect human intruders based on their body heat even in complete darkness?

- (A) Installing CCTV cameras with LED lights
- (B) Using ultrasonic motion sensors
- (C) Deploying infrared (IR) sensors
- (D) Implementing RFID badge readers at the entrance

Question 525. After a series of phishing attacks, the IT department of BetaTech Corp noticed that several employees were using easily guessable passwords. The security team decided to recommend the use of password managers to assist employees in creating and remembering strong passwords. Which of the following is a PRIMARY benefit of using password managers in this context?

- (A) Password managers automatically update the operating system
- (B) Password managers can generate and store complex

passwords

- (C) Password managers always prevent phishing attacks
- (D) Password managers allow the reuse of strong passwords across multiple platforms

Question 526. During a routine scan, the security team at a graphic design firm discovers that an employee downloaded an image from an email and subsequently, unusual network traffic was detected originating from that employee's workstation. The image appeared normal when opened. What type of attack might have been used in this situation?

- (A) Image Steganography Malware
- (B) Password Brute Force
- (C) Phishing
- (D) Port Scanning

Question 527. Acme Corp. is in the early stages of a potential lawsuit, and their legal department has just issued a notice for e-discovery related to email communications of a former executive. As an IT security professional, which of the following should be your FIRST action?

- (A) Start a full backup of the company's email server
- (B) Identify and isolate the email accounts related to the former executive
- (C) Immediately delete all emails that are more than two years old
- (D) Inform the media about the upcoming lawsuit

Question 528. A cloud-based e-commerce company wants to ensure that its inventory system automatically updates the stock levels on its website and third-party sales platforms whenever a

sale occurs. What should the company leverage to achieve this real-time synchronization?

- (A) Regularly backup the inventory system and restore it on the website and sales platforms
- (B) Rely on customers to report discrepancies in stock levels
- (C) Use Application Programming Interfaces (APIs) to integrate the inventory system with the website and third-party platforms
- (D) Conduct daily stock audits and manually update all platforms

Question 529. A financial organization's high-security data center has an authentication system for its main entry. If the system encounters an unexpected error, the organization wants to ensure that no one can gain access to the data center until the system is fixed. Which configuration should the authentication system be set to?

- (A) Fail-open
- (B) Fail-closed
- (C) Fail-secure
- (D) Fail-passive

Question 530. Jane, a security analyst, receives a report about network slowdowns happening at specific times of the day. After investigating, she discovers that a device is flooding the network with traffic, causing legitimate requests to be dropped. Which type of attack is this device likely performing?

- (A) Distributed Denial of Service (DDoS)
- (B) ARP poisoning
- (C) MAC flooding
- (D) DNS amplification

Question 531. A medium-sized financial firm has noticed a series of unauthorized transactions moving funds from legitimate accounts to overseas locations. After investigating, it was found that a group was responsible for exploiting vulnerabilities in the firm's transaction system. Which of the following motivations is most likely driving this group's actions?

- (A) Seeking notoriety within the hacker community
- (B) Financial gain from unauthorized transactions
- (C) Demonstrating political beliefs against financial institutions
- (D) Espionage to uncover the firm's investment strategies

Question 532. Country A and Country B are engaged in an ongoing territorial dispute. Suddenly, critical infrastructure facilities in Country B, such as power plants and transportation hubs, experience systematic cyberattacks. No ransom demand is made, and the attacks lead to significant disruption. What is the most probable motivation behind these cyberattacks?

- (A) Financial gain from market disruptions
- (B) Ethical hackers testing vulnerabilities
- (C) Disruption due to philosophical disagreements with Country B's policies
- (D) Acts of cyberwarfare to weaken Country B's position

Question 533. Alex, an employee at XYZ Corp, noticed an unfamiliar USB drive lying in the company parking lot. Out of curiosity, Alex plugged the device into his workstation. Almost immediately, his antivirus program detected malicious software trying to execute. What type of attack did Alex likely encounter?

- (A) Man-in-the-Middle Attack
- (B) Evil Twin
- (C) Spear Phishing
- (D) USB Drop Attack

Question 534. A company is setting up a secure communication channel between its headquarters and a remote branch office. To ensure that data transmitted over this channel originates from a legitimate system at the branch office, the company is considering using digital certificates. Which authentication method for systems is the company contemplating?

- (A) Kerberos authentication
- (B) Password-based authentication
- (C) Certificate-based authentication
- (D) Biometric-based authentication

Question 535. BioGen Inc., a biotechnology company, has implemented a layered security approach. They are considering adding a human element to their security measures for their research labs. Which of the following would best provide the ability to evaluate and respond to various security situations with human judgment?

- (A) Installing biometric locks
- (B) Employing security guards
- (C) Implementing an access control vestibule
- (D) Deploying AI-driven security cameras

Question 536. An environmental NGO's website was hacked and replaced with a message decrying their recent campaign against deforestation, claiming they are spreading misinformation. The website was left with a manifesto

promoting responsible forestry and sustainable logging practices. Which type of threat actor is MOST likely behind this incident?

- (A) Ransomware gang
- (B) Organized crime syndicate
- (C) Hacktivist
- (D) Advanced Persistent Threat (APT)

Question 537. After a major data breach in XYZ Corporation, the management decided to understand the primary reason behind the incident to prevent such occurrences in the future. Which of the following approaches should the incident response team prioritize to determine the fundamental cause of the breach?

- (A) Perform vulnerability scanning on all servers
- (B) Review firewall logs for the past week
- (C) Conduct a root cause analysis
- (D) Upgrade all security software

Question 538. AlphaCorp is migrating to cloud infrastructure and wants to ensure all virtual machines (VMs) are securely configured from the onset. Before deploying multiple VM instances, what should AlphaCorp do to ensure each VM starts from a secure configuration?

- (A) Use the default VM templates provided by the cloud provider
- (B) Establish a secure baseline for VM configurations and use it for deployment
- (C) Regularly backup all VMs
- (D) Use multi-factor authentication for cloud access

Question 539. An employee receives a call from someone claiming to be from the IT department. The caller says there's an urgent update required on the employee's computer and asks for login credentials to perform the update remotely. The employee becomes suspicious because of which red flag regarding impersonation?

- (A) The caller did not use technical jargon
- (B) IT normally sends email notifications about updates
- (C) The employee was not expecting any updates
- (D) The caller's voice sounded unfamiliar

Question 540. An organization with a single physical network infrastructure wants to separate the traffic of its finance department from that of the HR department. They do not want to set up entirely new physical networks but want to ensure that data packets from one department do not mix with the other's. What should the organization implement?

- (A) Air-gapped network
- (B) DMZ (Demilitarized Zone)
- (C) VLAN (Virtual Local Area Network)
- (D) VPN (Virtual Private Network)

Question 541. After detecting suspicious activity on a network, a digital forensic analyst is dispatched to acquire data from a potential compromised system. The analyst decides to capture an image of the affected system's memory. This technique of capturing volatile data is particularly beneficial because:

- (A) It helps identify deleted files
- (B) It can capture data in real-time operations
- (C) It provides information on patch levels
- (D) It offers insights into firewall configurations

Question 542. A company has faced multiple instances of unauthorized individuals gaining access to their office premises. Which of the following preventive security controls would be MOST effective in preventing unauthorized physical access?

- (A) Implementing a log monitoring solution for network traffic
- (B) Installing video surveillance cameras at all entry and exit points
- (C) Conducting regular security awareness training for employees
- (D) Implementing a multi-factor authentication system for network access.

Question 543. A software development company is looking to migrate its legacy applications to a more modern infrastructure. They want to ensure the applications can be deployed consistently across multiple environments without the challenges of varying dependencies and configurations. Which approach would best achieve this goal?

- (A) Virtual Machine Deployment
- (B) Bare-Metal Deployment
- (C) Containerization
- (D) Serverless Computing

Question 544. While conducting a security assessment, Lucy found that a specific application crashes when she inputs a string that is much longer than what the input field is designed to handle. This could potentially allow her to execute arbitrary code in the application's context. What vulnerability is Lucy likely trying to exploit?

- (A) SQL Injection

- (B) Cross-Site Scripting (XSS)
- (C) Buffer Overflow
- (D) Directory Traversal

Question 545. A major pharmaceutical company recently announced an increase in drug prices. Following the announcement, their website was taken offline by a DDoS attack, with a message posted online by a group claiming responsibility and demanding affordable healthcare for all. Which type of threat actor is MOST likely behind this attack?

- (A) Unskilled attacker
- (B) Insider threat
- (C) Hacktivist
- (D) Nation-state

Question 546. After a security breach, Jake, a digital forensics investigator, arrives at the scene to collect a hard drive for examination. He labels the hard drive, records its serial number, photographs the scene, and ensures the hard drive is transported securely to the forensics lab. These steps are crucial to:

- (A) Preserve the data's integrity on the hard drive
- (B) Maintain the chain of custody
- (C) Decrypt the data on the hard drive
- (D) Implement a legal hold on the data

Question 547. A security analyst has been tasked with investigating a possible data breach. While reviewing the network logs, the analyst noticed an unusual increase in outbound traffic to an unfamiliar IP address during non-business hours. The traffic appears to be encrypted and is associated with a known server containing sensitive data. Which of the

following is the MOST likely explanation for this behavior?

- (A) The server is downloading patches
- (B) An employee is accessing the server remotely
- (C) A backup of the server is being performed
- (D) Data exfiltration is occurring

Question 548. XYZ Corporation recently faced a major power outage that affected their primary data center. During the incident, it was found that there was no clear guidance on the steps to maintain or quickly restore business operations. To address this, which of the following policies should XYZ Corporation prioritize implementing?

- (A) Data Classification Policy
- (B) Business Continuity Policy
- (C) Acceptable Use Policy
- (D) Network Segmentation Strategy

Question 549. During a suspected security incident involving unauthorized access to sensitive data, Jake, an IT administrator, immediately disconnected the affected server from the network. Later, a digital forensic expert criticized Jake's action. Which of the following is the MOST likely reason for the criticism?

- (A) Jake should have left the server connected to capture more evidence from the attacker
- (B) Jake should have immediately informed the company's legal department
- (C) Jake should have taken an image of the server's memory before disconnecting it
- (D) Jake should have updated the server's software to prevent further unauthorized access

Question 550. ExamsDigest Corp, a technology company, recently conducted a security assessment to align with industry best practices. The company's current security posture was compared to its desired future state, revealing discrepancies. Which of the following best describes the approach ExamsDigest Corp employed?

- (A) Vulnerability Assessment
- (B) Penetration Testing
- (C) Gap Analysis
- (D) Threat Modeling

Question 551. During an annual review, a company discovered that one of its critical systems had several unscheduled downtimes over the year. The CTO has recommended a move towards high availability architecture to address this. What is the PRIMARY concern when implementing high availability?

- (A) Ensuring that there are no single points of failure
- (B) Ensuring that the system is patched regularly
- (C) Implementing multi-factor authentication
- (D) Storing backups in multiple geographical locations

Question 552. A government agency experienced a cyber incident where its communication platforms were breached. The intruders were not interested in extracting sensitive data or causing disruptions but were observed to be silently monitoring diplomatic communications for an extended period. What was the likely motivation of the attackers?

- (A) To gain financial benefits from insider trading
- (B) Espionage to understand and anticipate diplomatic moves

- (C) Disgruntlement of an internal employee
- (D) An attempt to expand their cybercriminal network

Question 553. AlphaTech's IT department is rolling out a new authentication protocol for remote workers. As part of the multifactor authentication process, employees are required to provide information that is memorized and cannot be physically taken from them. Which of the following represents this type of authentication factor?

- (A) Fingerprint
- (B) Smart card
- (C) PIN
- (D) USB security key

Question 554. An IT department in a large corporation spends several hours each day manually deploying patches and updates to thousands of workstations. Which of the following solutions would BEST enhance the efficiency of this process and save time for the IT team?

- (A) Disable automatic updates and conduct monthly patching sessions
- (B) Implement an automated patch management system
- (C) Designate a dedicated team for patching that operates in shifts
- (D) Educate users to install updates on their own

Question 555. A large e-commerce platform is facing challenges during peak sale periods, where the influx of users causes slowdowns and occasional outages. Which of the following solutions would BEST improve scalability during these high-demand times?

- (A) Implement a centralized logging system
- (B) Employ auto-scaling cloud solutions
- (C) Increase the frequency of data backups
- (D) Mandate regular security training for employees

Question 556. Alex, a new intern at an IT company, wanted to access the internal company portal. Instead of typing “companyportal.com,” he accidentally typed “comapnyportal.com” and ended up on a site that looked identical but asked him to download a security certificate. This scenario best describes which type of attack?

- (A) Spear Phishing
- (B) Watering Hole Attack
- (C) Typosquatting
- (D) Man-in-the-Middle

Question 557. A cloud infrastructure team frequently receives performance alerts from various resources in the environment. They want to ensure that relevant teams are immediately informed and can act upon any resource that crosses a performance threshold. What is the BEST way to accomplish this?

- (A) Conduct a weekly meeting to review all performance alerts
- (B) Automate ticket creation for any resource that crosses the performance threshold and assign it to the relevant team
- (C) Send all performance alerts to the cloud infrastructure team's email for review
- (D) Disable performance monitoring to reduce alert fatigue

Question 558. A large corporation is investigating a potential insider threat incident. A security analyst is tasked with examining the OS-specific security logs of a Windows server where sensitive documents are stored. Which of the following entries in the logs would MOST likely indicate unauthorized access attempts?

- (A) Logs displaying Windows Update successful installations
- (B) Entries showing a large number of failed login attempts followed by a successful login from a user outside of regular business hours
- (C) Logs indicating scheduled disk defragmentation tasks
- (D) Entries detailing successful printer connections and print jobs

Question 559. A company wants to ensure that security incidents are detected and addressed as quickly as possible by on-duty personnel. Which of the following operational security controls would be BEST to implement for this purpose?

- (A) Deploying a Network Intrusion Prevention System (NIPS)
- (B) Establishing a 24/7 Security Operations Center (SOC)
- (C) Creating a company-wide security policy
- (D) Implementing end-to-end data encryption

Question 560. AlphaCorp's IT department is reviewing password policies and wants to adopt a strategy that enhances security. Which of the following password strategies would be the MOST secure?

- (A) Passwords should be at least 6 characters long, with no other requirements

- (B) Passwords should be at least 10 characters long and include both uppercase and lowercase letters
- (C) Passwords should be at least 8 characters long and include uppercase letters, lowercase letters, numbers, and special characters
- (D) Passwords should be at least 4 characters long and include a mix of uppercase and lowercase letters

Question 561. SecureTech Corp, a company dealing with sensitive client data, is redesigning its main office entrance to enhance security. They want to ensure that only one person gains access at a time, even if multiple people try to enter using a single authorized access badge. Which of the following would best serve this purpose?

- (A) CCTV Cameras
- (B) Mantrap
- (C) Biometric Scanners
- (D) Motion Detectors

Question 562. After a recent incident of vandalism, a corporate building is considering implementing security controls that would dissuade potential perpetrators. Which of the following would serve BEST as a deterrent control?

- (A) Encrypting all stored data
- (B) Installing biometric access controls on all entrances
- (C) Implementing regular data backups
- (D) Placing visible security signage indicating 24/7 surveillance

Question 563. After deploying a new version of your company's internal application, several users reported issues

with accessing specific features. To investigate the root cause, you decided to review the application logs. What entry in the logs would most directly indicate a software bug or error related to the recent deployment?

- (A) Entries showing successful user authentication timestamps
- (B) Entries detailing the number of transactions completed by the application
- (C) Entries with "ERROR" or "EXCEPTION" related to the specific feature being accessed
- (D) Entries showing routine data backup operations

Question 564. OmegaTech recently introduced an additional layer of security for its remote server access. Along with their usual passwords, employees now need to use a physical device they have with them to gain access. Which of the following represents this “something you have” factor in multifactor authentication?

- (A) Password hint
- (B) Facial recognition
- (C) Hardware token
- (D) Voice recognition

Question 565. A system administrator is setting up an authentication system for a new web application. Which of the following security controls falls under the technical category and ensures that users prove their identity before gaining access?

- (A) Implementing a security awareness training program
- (B) Conducting a background check for new employees

- (C) Using multi-factor authentication
- (D) Establishing a clean desk policy

Question 566. BetaTech is implementing a new authentication mechanism for its data center technicians. Instead of using key cards, technicians will now have to look into a device that maps a specific pattern to authenticate their identity. Which of the following is BetaTech likely implementing?

- (A) Password system
- (B) Retina scanning
- (C) Hardware token
- (D) Knowledge-based questions

Question 567. DataCenter Inc. is located in a region prone to protests and vandalism. They wish to enhance their perimeter security to deter potential intruders and make it visibly clear that unauthorized access is restricted. Which of the following physical security measures would be the most effective first line of defense for the company?

- (A) Sliding Doors
- (B) Security Cameras
- (C) High-security Fencing
- (D) Proximity Card Readers

Question 568. Alice wants to access a restricted online portal. The portal asks her to enter a unique username and a secret passphrase only she should know. This process helps the system ensure that Alice is who she claims to be. What security concept is the portal employing?

- (A) Authorization
- (B) Accounting

- (C) Multifactor authentication
- (D) Authentication

Question 569. Employees at a renowned software development firm frequently visit an industry-related forum to discuss the latest trends and technologies. Over the past month, several employees reported malware infections shortly after accessing the forum. An investigation suggests the forum was compromised to target the company's developers specifically. Which type of attack most accurately describes this scenario?

- (A) Spear Phishing
- (B) Watering Hole
- (C) Drive-by Download
- (D) Whaling

Question 570. A cybersecurity analyst at XYZ Corp is looking to deploy a system that appears to be vulnerable and enticing to attackers. The main goal is to study the tactics, techniques, and procedures (TTPs) of potential adversaries, without them realizing that they're interacting with a decoy. Which of the following would BEST meet this requirement?

- (A) Intrusion Detection System (IDS)
- (B) Firewall
- (C) Honeypot
- (D) VPN Concentrator

Question 571. A large financial organization wants to ensure that all employees understand the importance of cybersecurity and the role they play in safeguarding company assets. Which of the following managerial security controls will be MOST effective in achieving this?

- (A) Installing a firewall at the network perimeter
- (B) Regular security awareness training for employees
- (C) Deploying an Intrusion Detection System (IDS)
- (D) Encrypting all company data

Question 572. You are an IT security professional for a large corporation. After receiving reports about some users being unable to access external websites, you decided to review the firewall logs. Which of the following would be a PRIMARY indicator in the logs that a rule is blocking outbound traffic?

- (A) Multiple entries of the same external IP address being ALLOWED
- (B) Timestamps showing large gaps between entries
- (C) Entries showing DROP/REJECT action for outbound traffic to port 80 and 443
- (D) Logs showing inbound traffic from multiple unknown external IP addresses

Question 573. A digital forensics investigator has just concluded an investigation regarding a potential insider threat. Before presenting the findings to the organization's board, which of the following should the investigator ensure about the forensic report?

- (A) The report includes technical jargon to showcase the depth of the investigation
- (B) The report emphasizes the investigator's credentials and experience
- (C) The report provides a clear, concise summary of findings without unnecessary technical details
- (D) The report contains detailed logs of every action taken by the investigator

Question 574. The security team at WidgetCorp is trying to identify potential insider threats. They have set up a SIEM solution with a custom dashboard showing unusual activities. Which of the following dashboard views would be MOST effective for quickly identifying an employee uploading large amounts of proprietary data to an external cloud storage service?

- (A) Display of users who logged in during off-hours
- (B) Graph of highest network bandwidth users
- (C) List of most frequently used applications
- (D) Visualization of failed login attempts

Question 575. During a regular review of system logs, Alex, a security analyst, noticed an unusual pattern of network traffic originating from a single IP address. Instead of waiting for an automated system to flag this as suspicious, he decides to manually dive deeper into the data to identify any potential threats. What is Alex engaging in?

- (A) Incident management
- (B) Threat modeling
- (C) Threat hunting
- (D) Security monitoring

Question 576. OmegaTech's security team noticed an increase in account compromises. An internal investigation revealed that many employees have been using the same passwords across different company systems and applications. Which password best practice can OmegaTech enforce to mitigate this issue?

- (A) Encouraging users to change their passwords every month
- (B) Implementing an account lockout policy after three

failed login attempts

(C) Prohibiting password reuse for at least the last five password changes

(D) Mandating that passwords contain only alphabetical characters for simplicity

Question 577. A medium-sized company suffered a data breach. Investigations revealed that an attacker from a rival firm had exploited a misconfigured firewall to gain unauthorized access to the company's database. Based on the attributes of the actor, how would this threat actor be best described?

(A) Internal actor leveraging physical access

(B) Internal actor abusing privileges

(C) External actor using social engineering

(D) External actor exploiting technical vulnerabilities

Question 578. In a microservices architecture, each service should be designed with a specific principle to ensure it performs a specific task and interacts with other services through well-defined interfaces. What principle is this referring to?

(A) Principle of Least Privilege

(B) Single Responsibility Principle

(C) Open-Closed Principle

(D) Zero Trust Model

Question 579. A company's online retail website faces DDoS attacks that cause significant downtime. Their current setup relies on manual verification of traffic spikes before mitigation efforts are deployed. What change could BEST enhance the company's reaction time to such attacks in the future?

- (A) Educate users to report slow website loading times
- (B) Manually back up the website data every hour
- (C) Deploy a web application firewall with automated DDoS mitigation features
- (D) Increase the website's bandwidth to handle traffic spikes

Question 580. A large enterprise is deploying a new automation system that will allow various teams, including development, operations, and QA, to provision and configure their own environments. The security team is concerned about potential misconfigurations or excessive permissions being granted. Which solution can be used within the automation to ensure security standards are met without limiting the agility of the teams?

- (A) Implementing a zero-trust model for all teams
- (B) Manually reviewing all requests before provisioning
- (C) Setting up guard rails within the automation scripts to define boundaries and prevent misconfigurations
- (D) Disabling the automation system for all teams except the security team

Question 581. SecureNet, a cybersecurity firm, is implementing an Intrusion Detection System (IDS) for its enterprise client. Where should the IDS be placed for optimal detection of malicious activities?

- (A) Before the perimeter firewall to capture all inbound traffic
- (B) Between the perimeter firewall and the internal network to monitor the filtered traffic
- (C) Inside the DMZ to monitor only external service

requests

(D) Adjacent to each workstation for personalized security

Question 582. AlphaTech wants to ensure that its remote employees follow best security practices when working from home. The security team has been tasked with drafting a set of guidelines for remote work. What should be the primary focus of these guidelines?

(A) Outlining punitive measures for non-compliance

(B) Stating the company's legal position on remote work

(C) Recommending security measures for home networks and devices

(D) Dictating the exact software and hardware specifications for remote workers

Question 583. The incident response team at XYZ Corp received a report that an attacker successfully exploited a vulnerable web application in their environment. To identify which server might have been compromised, the team decided to cross-reference recent vulnerability scan results. Which of the following information from the vulnerability scan would be MOST helpful in pinpointing the potentially compromised server?

(A) The timestamp of when the scan was conducted

(B) The software version of the scanning tool

(C) List of hosts with the specific vulnerability related to the exploit

(D) The total number of vulnerabilities identified during the scan

Question 584. While conducting a routine security review, Jake, a security specialist, discovers an unexpected piece of data placed in the organization's financial system. Upon asking, he learns that this piece of data is intentionally placed and monitored to see if any unauthorized user or system interacts with it. What is this deceptive piece of data known as?

- (A) Honeystring
- (B) Honeytoken
- (C) Canary token
- (D) Security marker

Question 585. DeltaCorp has a password policy in place which mandates users to change their passwords every 30 days. However, some users complain that this results in them choosing simpler passwords or writing them down to remember them. How can DeltaCorp maintain security while addressing these concerns?

- (A) Reduce the password change frequency but introduce more complexity requirements
- (B) Eliminate password changes and rely solely on two-factor authentication
- (C) Ask users to change passwords every week to improve security
- (D) Allow users to reuse any of their last three passwords to ease the transition

Question 586. A software company recently discovered a vulnerability in its popular application, which allowed unauthorized access to users' data. Before the company could release a patch, a group of hackers exploited the vulnerability but only to notify the users about it. They did not misuse any

data. What is the most probable motivation behind this group's action?

- (A) Financial gain by selling the data
- (B) Political beliefs against the software company's operations
- (C) Ethical concerns about user privacy and security
- (D) Desire to disrupt the software company's services

Question 587. In a routine security assessment, Claire found that a newly deployed database server within her organization is still using its default login credentials. Which of the following is the PRIMARY security risk associated with this finding?

- (A) The database will not function optimally
- (B) The server will need frequent patches
- (C) Unauthorized individuals may easily gain access
- (D) The server will consume more bandwidth

Question 588. DeltaTech, a progressive tech firm, is aiming to improve its security posture by eliminating the vulnerabilities associated with password use. They are considering deploying a passwordless authentication system. Which of the following represents the PRIMARY advantage of such a system?

- (A) It allows users to choose any password complexity
- (B) It eliminates the need for remembering passwords
- (C) It guarantees protection against all cyber threats
- (D) It ensures compatibility with all legacy systems

Question 589. A financial institution recently discovered that a large number of confidential customer records were being accessed and copied during off-business hours. Upon investigation, it was found that the access came from an

authenticated user within the company, who had recently been passed over for a promotion. Which type of threat actor is MOST likely responsible for this security incident?

- (A) Hacktivist
- (B) Insider threat
- (C) Nation-state
- (D) Organized crime syndicate

Question 590. A financial institution wants to ensure that customers are aware of the bank's policies on information sharing and how their personal data is used. Which of the following security controls would BEST communicate this to customers?

- (A) Implementing end-to-end encryption for online transactions
- (B) Publishing a privacy policy on the bank's website
- (C) Conducting annual cybersecurity awareness training for employees
- (D) Using multi-factor authentication for online banking

Question 591. OmegaHealth, a large healthcare provider, is integrating automation into its operations. When a new healthcare worker is hired, they require access to multiple systems. Why would OmegaHealth automate the user provisioning process across these systems?

- (A) To enforce a uniform password for all healthcare workers.
- (B) To save time by ensuring consistent and simultaneous account creation across all necessary platforms
- (C) To prevent the new hires from accessing any system until their probation period ends

(D) To reduce the software licenses needed by delaying account activation

Question 592. After detecting an unauthorized intrusion into their network, a financial institution wants to implement a control that will restore compromised systems to a known good state. Which of the following would be the MOST appropriate corrective control?

- (A)** Implementing Intrusion Detection Systems (IDS) across the network
- (B)** Frequently updating firewall rules
- (C)** Restoring systems from verified backups
- (D)** Enabling multi-factor authentication for users

Question 593. Maria receives a text message on her phone from an unknown number, stating that she has won a gift card worth \$500 from a popular online store. The message includes a link asking her to click on it to claim her prize. Maria is unsure about the authenticity of the message. Which of the following is the BEST course of action for Maria?

- (A)** Click the link to check if the website looks genuine
- (B)** Forward the message to her friends to verify if they received a similar message
- (C)** Delete the message without clicking on any links
- (D)** Respond to the sender asking for more details about the offer

Question 594. In preparation for a potential lawsuit, Meg, a cybersecurity analyst, has been asked to ensure that specific digital evidence remains intact and is not altered or deleted. What measure should Meg implement to ensure this

requirement?

- (A) Encrypt the evidence
- (B) Initiate a legal hold
- (C) Perform a full disk wipe
- (D) Conduct a vulnerability assessment

Question 595. In an IaaS (Infrastructure as a Service) model, which of the following tasks is typically the responsibility of the cloud customer in a standard Cloud Responsibility Matrix?

- (A) Physical security of data centers
- (B) Patching of host operating systems
- (C) Network infrastructure maintenance
- (D) Patching of guest operating systems

Question 596. A company detected a DDoS attack that lasted for several weeks. The attackers used a botnet of millions of infected devices and frequently rotated attack vectors to bypass mitigation efforts. This prolonged and resource-intensive attack suggests which kind of threat actor's resources and funding?

- (A) Amateur hacker with minimal resources
- (B) Cybersecurity researcher testing vulnerabilities
- (C) Nation-state actor with strategic interests
- (D) Organized crime syndicate with substantial funding

Question 597. An art gallery wants to deploy a security solution to detect movement in an open courtyard that features several sculptures. This space has varying temperature conditions, which might cause false alarms in some motion detection technologies. Which type of sensor would be MOST appropriate to ensure consistent motion detection in such conditions?

- (A) Thermal imaging sensors
- (B) Pressure-sensitive mats
- (C) Ultrasonic detectors
- (D) Microwave motion detectors

Question 598. TechBlitz Inc. recently underwent an IT audit, and one of the suggestions was to reduce the attack surface. Which of the following measures would be MOST effective in accomplishing this?

- (A) Increasing the password length requirement for all users
- (B) Implementing regular vulnerability assessments
- (C) Deactivating unused services and ports on servers
- (D) Implementing a strict BYOD (Bring Your Own Device) policy

Question 599. A user receives an SMS claiming to be from her bank, alerting her of unauthorized activity on her account. The message instructs the user to immediately click on a provided link and verify her account details. The user hasn't noticed any irregularities with her bank account. Which type of attack is this SMS most likely part of?

- (A) Smishing
- (B) Vishing
- (C) Bluejacking
- (D) Bluesnarfing

Question 600. After a recent security breach, CyberCorp is reviewing its software vendors for their responsiveness to vulnerabilities. Which of the following metrics would BEST

assist CyberCorp in determining the timeliness and efficiency of security patches from a vendor?

- (A) The frequency of software updates released by the vendor
- (B) The vendor's quarterly financial reports
- (C) Time between vulnerability disclosure and patch release by the vendor
- (D) The number of features added by the vendor in the last software update

Answers 501-600

Question 501. A company's website was temporarily defaced with a humorous meme, but no sensitive data was stolen or any significant damage done. The attacker left a message bragging about their first successful hack. Which type of threat actor is MOST likely responsible for this attack?

- (A) Insider threat
- (B) Advanced Persistent Threat (APT)
- (C) **Unskilled attacker**
- (D) Nation-state

Explanation 501. Correct Answer: C. Unskilled attacker.

Unskilled attackers, often referred to as “script kiddies”, typically utilize pre-made tools or scripts to carry out basic attacks. Their motivations are often more about bragging rights or minor mischief, such as defacing a website for fun or to prove they can, rather than executing a sophisticated or damaging attack.

Option A is incorrect. Insider threats are individuals within an organization that may have specific motives related to personal grievances or financial gain. Their attacks would typically be more targeted and potentially more harmful than just defacing a website.

Option B is incorrect. Advanced Persistent Threats (APTs) are highly skilled and typically represent organized groups with specific, long-term objectives. Their attacks are sophisticated

and stealthy, aiming for data theft or system compromise over an extended period.

Option D is incorrect. Nation-states are motivated by political, military, or espionage objectives. A simple website defacement, especially one with a humorous meme, does not align with their typical motivations or methods.

Question 502. A financial institution has experienced an uptick in unauthorized transactions. They want to implement a control that will allow them to identify suspicious transactions in real-time. Which of the following would be the BEST detective control for this scenario?

- (A) Implementing a multi-factor authentication system for all users
- (B) Establishing a Security Operations Center (SOC) to monitor network traffic
- (C) **Installing an Intrusion Detection System (IDS) on their network**
- (D) Restricting transaction capabilities to only a few trusted IP addresses.

Explanation 502. Correct Answer: C. Installing an Intrusion Detection System (IDS) on their network. An Intrusion Detection System (IDS) serves as a detective control by monitoring network traffic for suspicious activities and potential threats. In this context, it can be configured to detect patterns related to unauthorized transactions, thereby allowing timely intervention.

Option A is incorrect. Implementing a multi-factor authentication system is a preventive control that provides an additional layer of security by requiring two or more verification methods. While it reduces the risk of unauthorized access, it does not detect suspicious transactions.

Option B is incorrect. Establishing a Security Operations Center (SOC) is a broad approach to handle security events, and while it can include detective controls, merely setting up a SOC does not provide specific real-time detection of unauthorized transactions.

Option D is incorrect. Restricting transaction capabilities to only a few trusted IP addresses is a preventive control that limits the sources of potential transactions. While it can reduce the number of unauthorized transactions, it does not detect them.

Question 503. GammaTech has a new remote access policy for its employees. Whenever an employee attempts to access the corporate network from an unfamiliar location, the system requests additional verification before granting access. Which factor of authentication is being emphasized in this policy?

- (A) Knowledge-based questions the employee answers
- (B) A fingerprint scan from the employee
- (C) **The physical coordinates of the employee's access point**
- (D) An SMS code sent to the employee's phone

Explanation 503. Correct Answer: C. The physical coordinates of the employee's access point. By verifying the

location or coordinates of an access point, GammaTech is utilizing the “somewhere you are” factor in multifactor authentication. This emphasizes the geographic location of the user.

Option A is incorrect. Knowledge-based questions fall under the “something you know” factor since users answer based on information they recall.

Option B is incorrect. A fingerprint scan pertains to the “something you are” factor as it’s a biometric, a unique physical characteristic of the individual.

Option D is incorrect. An SMS code sent to a phone belongs to the “something you have” factor, as it’s sent to a device in the user’s possession.

Question 504. The cybersecurity team of XYZ Corp. plans to assess their organization’s preparedness for a potential data breach. They aim to evaluate the effectiveness of their response strategy without performing any real actions. Which of the following methods would BEST help them achieve this goal?

- (A) Live fire exercise
- (B) System hardening test
- (C) Red team/blue team exercise
- (D) **Tabletop exercise**

Explanation 504. Correct Answer: D. Tabletop exercise. A tabletop exercise is a discussion-based session where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular

emergency situation. It allows for an assessment of an incident response strategy without performing any actual tasks.

Option A is incorrect. A live fire exercise is a real-world test, often unannounced, and could impact actual operations.

Option B is incorrect. System hardening test focuses on making a system more secure against attacks and does not evaluate incident response.

Option C is incorrect. Red team/blue team exercises involve simulating real-world cyber attacks to test an organization's defense and response capabilities, which is more hands-on than what is described.

Question 505. A company is attempting to verify the legitimacy of an email sent from a senior executive to a number of employees. The email requests the recipients to click on a link and enter their credentials for a "system upgrade." The security team wants to ascertain if the email genuinely came from the executive. Which of the following metadata from the email would be MOST beneficial in this investigation?

- (A) The email's subject line
- (B) The email's send time and date
- (C) **The originating IP address in the email headers**
- (D) The size of the email in bytes

Explanation 505. Correct Answer: C. The originating IP address in the email headers. Email headers often contain metadata about the originating IP address of the email. This can help investigators determine if the email was sent from an

expected location or if it originated from an unfamiliar or suspicious IP, indicating a possible phishing attempt.

Option A is incorrect. The subject line of an email is not typically indicative of its authenticity.

Option B is incorrect. While knowing the send time and date may provide some context, it won't necessarily verify the legitimacy of the email sender.

Option D is incorrect. The size of the email in bytes doesn't offer significant value in determining the authenticity of the email's origin.

Question 506. An online banking website employs a system that automatically logs out users after 10 minutes of inactivity to ensure that if a user forgets to log out, no one else can alter the user's banking details. Which principle of the CIA triad is the banking website MOST directly addressing?

- (A) Confidentiality
- (B) Availability
- (C) Authentication
- (D) **Integrity**

Explanation 506. Correct Answer: D. Integrity. The integrity pillar of the CIA triad ensures the accuracy and reliability of data. By logging out users after a period of inactivity, the banking website aims to prevent unauthorized modifications (potentially by someone else who might gain access to the unattended session) to the user's banking details, thereby maintaining the integrity of the data.

Option A is incorrect. While logging out users does have a confidentiality aspect, the primary aim in this scenario is to prevent unauthorized changes rather than unauthorized viewing.

Option B is incorrect. Availability ensures that data and systems are accessible to authorized users when they need it. This scenario doesn't discuss providing or restricting access based on system uptime or accessibility.

Option C is incorrect. Authentication ensures that users are who they claim to be. While the scenario does touch on security measures, the primary concern here is preventing unauthorized changes to data, which aligns with integrity, not authentication

Question 507. An IT department in a large corporation spends several hours each day manually deploying patches and updates to thousands of workstations. Which of the following solutions would BEST enhance the efficiency of this process and save time for the IT team?

- (A) Disable automatic updates and conduct monthly patching sessions
- (B) **Implement an automated patch management system**
- (C) Designate a dedicated team for patching that operates in shifts
- (D) Educate users to install updates on their own

Explanation 507. Correct Answer: B. Implement an automated patch management system. By implementing an automated patch management system, the IT department can streamline the deployment of patches and updates across all

workstations, ensuring consistency, reducing manual efforts, and saving valuable time.

Option A is incorrect. Disabling automatic updates and conducting monthly patching sessions does not address the inefficiency of manual patching and might expose the systems to vulnerabilities for a longer time.

Option C is incorrect. While designating a dedicated team might distribute the workload, it doesn't eliminate the inefficiencies associated with manual patching.

Option D is incorrect. Relying on users to install updates introduces inconsistency, potential delays, and additional risks, as not all users might have the technical knowledge or remember to update regularly.

Question 508. Epsilon Inc. recently hired Jenny as a junior network administrator. To ensure security, they give Jenny only the access permissions necessary to complete her specific tasks, such as monitoring network traffic, but not modifying firewall rules. This approach of granting Jenny's permissions aligns with which security principle?

- (A) Mandatory Access Control (MAC)
- (B) Role-Based Access Control (RBAC)
- (C) Time-of-Day Restrictions
- (D) **Least Privilege**

Explanation 508. Correct Answer: D. Least Privilege. The principle of Least Privilege dictates that users should be granted the minimum levels of access – or the least amount of privileges

– necessary to complete their job functions. In Jenny’s case, she’s only granted the permissions necessary for her role, which aligns with this principle.

Option A is incorrect. MAC involves classifying information and matching user clearance levels to these classifications. Jenny’s access isn’t based on classifications.

Option B is incorrect. RBAC assigns permissions based on roles within an organization. While Jenny’s permissions may be aligned with her role, the scenario specifically emphasizes granting the minimal necessary access, which is a characteristic of Least Privilege.

Option C is incorrect. Time-of-Day Restrictions determine access based on the current time and have no direct relation to the principle of Least Privilege.

Question 509. As part of a cloud infrastructure project, AlphaTech plans to deploy multiple virtualized resources for its new application. The deployment includes databases, web servers, and load balancers. What is the PRIMARY benefit of using automation scripts in the resource provisioning process for this project?

- (A) It enables AlphaTech to use a single operating system for all resources
- (B) It guarantees 100% uptime for all virtualized resources
- (C) **It ensures standardized, repeatable, and rapid deployments across the infrastructure**
- (D) It prevents unauthorized users from accessing the cloud infrastructure

Explanation 509. Correct Answer: C. It ensures standardized, repeatable, and rapid deployments across the infrastructure. Automation in resource provisioning provides consistency in deployments, allowing for standardized configurations, rapid scaling, and the ability to repeat deployments without human error.

Option A is incorrect. While automation can deploy similar or consistent environments, it does not inherently enforce a single operating system.

Option B is incorrect. Automation can increase efficiency and reduce human errors, but it cannot guarantee 100% uptime, as there are other factors involved, like hardware failures or network issues.

Option D is incorrect. While automation can implement security configurations, it does not, by itself, prevent unauthorized access. Security measures need to be designed and implemented separately.

Question 510. CyberSec Corp's CISO wants to determine if there have been any anomalies in user behavior over the past month. Specifically, they're concerned about unauthorized data transfers outside of regular business hours. Which of the following automated reports would be MOST useful in this investigation?

- (A) **After-hours network activity reports**
- (B) User password change frequency reports
- (C) Hardware inventory audit reports
- (D) Software licensing compliance reports

Explanation 510. Correct Answer: A. After-hours network activity reports. For the specific concern of unauthorized data transfers outside of regular business hours, the after-hours network activity reports would be most useful. These reports would provide details on network activities, including data transfers, that took place outside typical working hours.

Option B is incorrect. While user password change frequency reports might indicate if users are frequently changing passwords, which could be a sign of suspicious activity, it wouldn't directly address the concern of data transfers outside of regular hours.

Option C is incorrect. Hardware inventory audit reports would provide information about the hardware assets of the company but wouldn't give insights into data transfer activities.

Option D is incorrect. Software licensing compliance reports would detail the compliance status of software licenses, which isn't relevant to the concern about unauthorized data transfers after hours.

Question 511. During a review of IDS logs, a security specialist notices a series of alerts indicating that a single external IP has been sending payloads that exploit a known vulnerability. However, the internal system to which these payloads are sent is patched and is not vulnerable to the exploit. Which of the following describes this type of IDS alert?

(A) False positive

(B) False negative

- (C) True positive
- (D) True negative

Explanation 511. Correct Answer: C. True positive. A true positive means the IDS correctly identified malicious or anomalous traffic. In this case, even though the internal system isn't vulnerable, the IDS correctly flagged the traffic because it's genuinely malicious.

Option A is incorrect. A false positive would mean the IDS incorrectly flagged benign traffic as malicious, which is not the case here.

Option B is incorrect. A false negative means the IDS failed to identify malicious or anomalous traffic, but in this scenario, the IDS did correctly identify the malicious traffic.

Option D is incorrect. A true negative means the IDS correctly identified benign traffic as benign. The traffic in this scenario was malicious, so this doesn't apply.

Question 512. An organization recently experienced a malware infection on one of its workstations. A security analyst has been tasked with reviewing the endpoint logs of the infected system to gather more information about the incident. Which of the following entries in the endpoint logs would be MOST indicative of the initial malware infection point?

- (A) Logs indicating successful user login and logout events
- (B) Entries showing periodic system health-check status as "OK"
- (C) Logs documenting a recently installed and executed

unknown .exe file from a temporary directory

(D) Entries detailing network connectivity checks to the domain controller

Explanation 512. Correct Answer: C. Logs documenting a recently installed and executed unknown .exe file from a temporary directory. Endpoint logs that document the installation and execution of an unknown .exe file, especially from a temporary directory, are strong indicators of potentially malicious activity. Such logs can pinpoint the initial infection point of malware on a system.

Option A is incorrect. User login and logout events are routine logs and do not provide specific information about malware infections unless associated with other suspicious activities.

Option B is incorrect. System health-check status entries are meant to provide general information about the system's health and do not specify actions or changes made on the system related to malware.

Option D is incorrect. Network connectivity checks to domain controllers are routine in many network environments and don't directly indicate malware activity.

Question 513. A security analyst is reviewing the IPS logs and discovers multiple alerts originating from a single IP address attempting to access various company servers. The analyst is trying to determine the type of attack. Which of the following log entries BEST indicates a port scanning activity?

(A) Multiple consecutive connection attempts to different

ports on a single server in a short time frame

- (B) Repeated connection attempts to port 80 of a web server every 3 seconds
- (C) Numerous failed login attempts to an FTP server from the same IP address
- (D) Consistent pings to the network gateway every 5 seconds

Explanation 513. Correct Answer: A. Multiple consecutive connection attempts to different ports on a single server in a short time frame. Port scanning is an activity where an attacker probes a server or host to determine what services are running. Rapid connection attempts to various ports indicate that the attacker is trying to discover open ports and the services running on them.

Option B is incorrect. While repeated connection attempts to a single port could be suspicious, it doesn't indicate port scanning. This could be indicative of a DoS attack.

Option C is incorrect. Multiple failed login attempts indicate a possible brute force attack on the FTP server, not port scanning.

Option D is incorrect. Regular pings to the network gateway might be indicative of network mapping or checking connectivity but doesn't suggest port scanning activity.

Question 514. A global financial company experiences sporadic cyber attacks on its infrastructure. The company notices that attacks that occur during non-business hours often result in more significant damage due to delayed responses. Which of the

following measures would BEST decrease the reaction time to these off-hour attacks?

- (A) **Multiple consecutive connection attempts to different ports on a single server in a short time frame**
- (B) Repeated connection attempts to port 80 of a web server every 3 seconds
- (C) Numerous failed login attempts to an FTP server from the same IP address
- (D) Consistent pings to the network gateway every 5 seconds

Explanation 514. Correct Answer: A. Multiple consecutive connection attempts to different ports on a single server in a short time frame. Port scanning is an activity where an attacker probes a server or host to determine what services are running. Rapid connection attempts to various ports indicate that the attacker is trying to discover open ports and the services running on them.

Option B is incorrect. While repeated connection attempts to a single port could be suspicious, it doesn't indicate port scanning. This could be indicative of a DoS attack.

Option C is incorrect. Multiple failed login attempts indicate a possible brute force attack on the FTP server, not port scanning.

Option D is incorrect. Regular pings to the network gateway might be indicative of network mapping or checking connectivity but doesn't suggest port scanning activity.

Question 515. GreenTech, a data center company, is planning to expand its operations in a region known for frequent power outages. To maintain security posture and ensure continuity of operations, which of the following should be their PRIMARY consideration regarding power?

- (A) Using power-efficient servers to reduce electricity costs
- (B) Setting up solar panels to promote green energy
- (C) **Investing in redundant power supplies and uninterruptible power systems (UPS)**
- (D) Running operations only during peak daylight hours to ensure natural lighting

Explanation 515. Correct Answer: C. Investing in redundant power supplies and uninterruptible power systems (UPS). Given the frequent power outages in the region, having redundant power supplies and UPS ensures that operations continue smoothly without abrupt interruptions, which can lead to system crashes, data corruption, or security breaches.

Option A is incorrect. While power-efficient servers can reduce costs, they do not address the primary concern of power outages and maintaining operations.

Option B is incorrect. Solar panels promote green energy but might not provide consistent and immediate power backup during outages, especially during nighttime or cloudy days.

Option D is incorrect. Limiting operations to daylight hours is not a practical solution for a data center, as it restricts

operational capacity and doesn't directly address the issue of power outages.

Question 516. A medium-sized enterprise is concerned about the security of its office workstations after a series of malware infections. As a security analyst, which of the following recommendations would BEST improve the security baseline of the workstations?

- (A) Install multiple antivirus solutions to ensure maximum detection
- (B) Set up screensavers with cyber hygiene tips to educate users
- (C) **Disable unnecessary services and ports on the workstations**
- (D) Frequently change the desktop wallpaper to prevent monotony

Explanation 516. Correct Answer: C. Disable unnecessary services and ports on the workstations. By disabling unnecessary services and ports, you reduce the number of potential attack vectors and vulnerabilities, thus improving the security baseline of the workstations.

Option A is incorrect. Installing multiple antivirus solutions can lead to conflicts and may degrade system performance. It's better to have one robust, updated antivirus solution.

Option B is incorrect. While cyber hygiene tips can be informative, they don't directly contribute to the technical security baseline of a workstation.

Option D is incorrect. Changing the desktop wallpaper does nothing for security. Its primary purpose is aesthetics.

Question 517. A large financial institution is planning to upgrade its IT infrastructure to allow for a more efficient use of hardware resources, faster deployment of applications, and reduced server provisioning times. While evaluating different technologies, which of the following would directly address these needs?

- (A) Network Segmentation
- (B) Intrusion Detection System
- (C) **Virtualization**
- (D) Multi-Factor Authentication

Explanation 517. Correct Answer: C. Virtualization.

Virtualization allows multiple virtual machines to run on a single physical host, maximizing the use of hardware resources. It enables rapid provisioning and deployment of new servers and applications, addressing the requirements of the financial institution.

Option A is incorrect. Network segmentation divides a network into smaller subnetworks, primarily for security and performance reasons. While it's a best practice, it doesn't address the efficient use of hardware or rapid deployment of applications.

Option B is incorrect. An Intrusion Detection System (IDS) monitors and detects malicious activities in a network. While crucial for security, it doesn't cater to hardware resource efficiency or faster server provisioning.

Option D is incorrect. Multi-Factor Authentication is a security process in which a user provides multiple methods of identification to authenticate their identity. It doesn't impact hardware resource efficiency or application deployment times.

Question 518. The security team of a multinational company deployed a network of honeypots globally, making it appear as an interconnected and realistic environment. They aim to study coordinated multi-stage attacks. This deceptive setup is known as:

- (A) Firewall Cluster
- (B) Virtual LAN (VLAN)
- (C) Distributed Denial of Service (DDoS) Prevention
- (D) **Honeynet**

Explanation 518. Correct Answer: D. Honeynet. A honeynet is essentially a network of honeypots. It is designed to be attractive to attackers, making them believe they are attacking a real network, while in reality, they are being observed, and their tactics and techniques are being analyzed.

Option A is incorrect. A Firewall Cluster is a group of firewalls operating together to increase reliability and performance. It doesn't serve as a decoy to attract attackers.

Option B is incorrect. A Virtual LAN (VLAN) is a network protocol used to create logically segmented networks within a physical network, improving performance and security. It's not a decoy system.

Option C is incorrect. Distributed Denial of Service (DDoS) Prevention solutions focus on identifying and mitigating large-scale attempts to disrupt network service availability. They do not present a deceptive environment for attackers.

Question 519. Sophia, the CFO of a medium-sized company, received a call from an individual claiming to be from the IT department. The caller requested her login details for a “critical system update.” Suspecting something wasn’t right, Sophia hung up and contacted her IT department, which confirmed no such call was made by them. Which type of attack did Sophia most likely experience?

- (A) **Vishing**
- (B) Phishing
- (C) SQL Injection
- (D) Cross-Site Request Forgery (CSRF)

Explanation 519. Correct Answer: A. Vishing. Vishing, or voice phishing, is an attack where fraudsters use the telephone to mislead individuals into revealing personal information or login credentials.

Option B is incorrect. Phishing is typically an attempt to obtain sensitive information through deceptive emails and websites, not voice calls.

Option C is incorrect. SQL Injection is an attack type that tries to execute malicious SQL statements in a database. It is not related to voice calls.

Option D is incorrect. Cross-Site Request Forgery (CSRF) is a type of attack where the attacker tricks the victim into submitting a malicious request. This is unrelated to voice call scenarios.

Question 520. Sophia received an email from her bank asking her to urgently update her personal details due to a system upgrade. The email contains a link that redirects to a website that looks similar to her bank's website. Which of the following should she do FIRST?

- (A) Follow the link and promptly update her personal details to avoid any inconvenience
- (B) Forward the email to her friends and family to ensure they are also aware of the bank's system upgrade
- (C) Delete the email immediately without taking any action
- (D) **Contact her bank through official channels to verify the authenticity of the email**

Explanation 520. Correct Answer: D. Contact her bank through official channels to verify the authenticity of the email. Before taking action based on an unsolicited email, especially one that asks for personal information or credentials, it's essential to verify its legitimacy directly with the institution or entity it claims to represent.

Phishing attacks often use fear, urgency, or perceived authority to lure victims into providing sensitive data. The best defense against such attempts is to independently verify any unexpected or suspicious requests before taking action.

Option A is incorrect. Directly responding to a potential phishing email by providing personal details is a common mistake, making the user vulnerable to fraud and identity theft.

Option B is incorrect. Forwarding a potentially malicious email to others can further propagate the threat and possibly compromise their security as well.

Option C is incorrect. While deleting the email might prevent Sophia from falling for the phishing attempt, it's still a good practice to inform the bank about the suspicious email so they can take appropriate measures and warn other customers.

Question 521. Tech Enterprises is planning to release a new product. As part of the product's creation, they've sourced components from various vendors. The security team is tasked with assessing risks linked to the supply chain. Which of the following is the MOST concerning risk when sourcing components from multiple vendors?

- (A) Difficulty in tracking product warranty details from multiple vendors
- (B) Increased product assembly time due to varied vendor delivery timelines
- (C) **Potential for introduction of insecure or compromised components**
- (D) The need for multiple purchase orders, leading to increased paperwork

Explanation 521. Correct Answer: C. Potential for introduction of insecure or compromised components. When components are sourced from multiple vendors, there is a

heightened risk that one or more components might have vulnerabilities or could be compromised, thus impacting the security of the overall product.

The integrity and security of components are vital in product development, especially when those components are part of the supply chain from various vendors. If one vendor has lax security measures or gets compromised, the components they supply can introduce vulnerabilities into the finished product, affecting its overall security posture and potentially leading to data breaches or other cyber threats.

Option A is incorrect. While tracking warranties is an operational concern, it doesn't pose a direct security risk when sourcing components from multiple vendors.

Option B is incorrect. Product assembly time and vendor delivery timelines are logistical and operational concerns, not primary security risks associated with supply chain vendors.

Option D is incorrect. Managing multiple purchase orders is a business process challenge, not a primary security concern.

Question 522. ThetaTech, a financial institution, wants to upgrade its authentication system for high-net-worth customers accessing their accounts online. Besides the traditional password, they want to include a method that captures unique physical or behavioral characteristics. Which type of authentication method should ThetaTech consider?

- (A) Token-based authentication
- (B) Geolocation tracking

- (C) Biometrics
- (D) Smart card

Explanation 522. Correct Answer: C. Biometrics. Biometrics authentication involves recognizing an individual based on their unique physical or behavioral characteristics, such as fingerprints, retina scans, or voice recognition.

Option A is incorrect. Token-based authentication provides users with a device or software token that generates a time-sensitive code. It doesn't capture physical or behavioral characteristics.

Option B is incorrect. Geolocation tracking determines a user's location but doesn't involve capturing unique physical or behavioral traits.

Option D is incorrect. A smart card is a physical card that contains electronic information. It can be used for authentication, but it does not inherently capture unique physical or behavioral characteristics.

Question 523. A software development team in a large corporation decided to use an unauthorized cloud-based tool to host and manage their source code. The team believed it would increase their productivity, even though it was not approved by the IT department. A few weeks later, unauthorized access to their project data was detected. Which threat actor concept BEST describes the situation?

- (A) Insider threat
- (B) Hacktivist

- (C) Shadow IT
- (D) Organized crime syndicate

Explanation 523. Correct Answer: C. Shadow IT. Shadow IT refers to any IT systems or solutions used within an organization without organizational approval or oversight. This can introduce vulnerabilities, as the unauthorized systems might not meet the security standards set by the organization's IT department. In this scenario, the software development team's unauthorized use of a cloud tool exemplifies Shadow IT.

Option A is incorrect. While the software development team acted without approval, their intention was to increase productivity, not to harm the organization. Therefore, this situation does not fit the typical definition of an "insider threat," which usually has malicious intent.

Option B is incorrect. Hacktivists are motivated by political or social causes. There's no evidence in the scenario to suggest that political or social motivations were behind the team's decision.

Option D is incorrect. While the data was accessed without authorization, there's no evidence to suggest that this was the work of an organized crime syndicate. The main issue at hand is the unauthorized use of IT resources, which is a hallmark of Shadow IT.

Question 524. TechHaus has recently experienced multiple security breaches where unauthorized personnel have managed to infiltrate their server rooms after hours. To enhance security

measures, the company decided to deploy a new system. Which of the following options would BEST detect human intruders based on their body heat even in complete darkness?

- (A) Installing CCTV cameras with LED lights
- (B) Using ultrasonic motion sensors
- (C) **Deploying infrared (IR) sensors**
- (D) Implementing RFID badge readers at the entrance

Explanation 524. Correct Answer: C. Deploying infrared (IR) sensors. Infrared (IR) sensors detect infrared radiation, such as the heat emitted by the human body. This makes them particularly effective in detecting human intruders, even in complete darkness, based on the body heat they emit.

Option A is incorrect. While CCTV cameras with LED lights can provide visual surveillance, they rely on light to produce images and may not detect intruders in complete darkness as efficiently as infrared sensors.

Option B is incorrect. Ultrasonic motion sensors detect movement through sound waves, not body heat, making them less efficient in differentiating between a human intruder and other moving objects.

Option D is incorrect. RFID badge readers control access at entry points but do not detect human intruders based on their body heat inside a facility.

Question 525. After a series of phishing attacks, the IT department of BetaTech Corp noticed that several employees were using easily guessable passwords. The security team

decided to recommend the use of password managers to assist employees in creating and remembering strong passwords.

Which of the following is a PRIMARY benefit of using password managers in this context?

- (A) Password managers automatically update the operating system
- (B) **Password managers can generate and store complex passwords**
- (C) Password managers always prevent phishing attacks
- (D) Password managers allow the reuse of strong passwords across multiple platforms

Explanation 525. Correct Answer: B. Password managers can generate and store complex passwords. Password managers can automatically generate complex passwords that meet a variety of criteria (e.g., length, use of special characters, avoidance of easily guessable terms) and store them securely. This helps users maintain strong, unique passwords for every service they use without needing to remember each one.

Option A is incorrect. Password managers are designed for generating, retrieving, and storing complex passwords, not for updating the operating system.

Option C is incorrect. While password managers can help reduce the risk of successful phishing attacks by storing passwords securely and autofilling them on recognized websites, they don't always prevent phishing attacks, especially if a user is deceived into entering credentials on a fake website.

Option D is incorrect. One of the primary benefits of password managers is to ensure that users have unique passwords for each application or service. Reusing passwords, even if strong, across multiple platforms poses a security risk.

Question 526. During a routine scan, the security team at a graphic design firm discovers that an employee downloaded an image from an email and subsequently, unusual network traffic was detected originating from that employee's workstation. The image appeared normal when opened. What type of attack might have been used in this situation?

- (A) **Image Steganography Malware**
- (B) Password Brute Force
- (C) Phishing
- (D) Port Scanning

Explanation 526. Correct Answer: A. Image Steganography Malware. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. Image steganography specifically involves hiding malicious code within an image. When the image is downloaded or opened, the malicious code can be executed without the victim's knowledge.

Option B is incorrect. Password Brute Force is an attack method where an attacker attempts to guess a user's password by systematically trying every possible combination of letters, numbers, and symbols until the correct password is discovered.

Option C is incorrect. Phishing typically involves deceptive emails or messages attempting to trick recipients into divulging

sensitive information. While images can be used in phishing attempts, the scenario described does not indicate an attempt to extract information from the employee.

Option D is incorrect. Port Scanning is an attempt to discover open ports on a computer, which can reveal services running on those ports. It does not involve the use of images.

Question 527. Acme Corp. is in the early stages of a potential lawsuit, and their legal department has just issued a notice for e-discovery related to email communications of a former executive. As an IT security professional, which of the following should be your FIRST action?

- (A) Start a full backup of the company's email server
- (B) **Identify and isolate the email accounts related to the former executive**
- (C) Immediately delete all emails that are more than two years old
- (D) Inform the media about the upcoming lawsuit

Explanation 527. Correct Answer: B. Identify and isolate the email accounts related to the former executive. In the context of e-discovery, it's crucial to locate and preserve electronically stored information (ESI) that could be relevant to the lawsuit. The first step would be to identify and isolate the specific email accounts or data sources relevant to the request to ensure they are not tampered with or deleted.

Option A is incorrect. While backups are essential, a blanket backup of the email server may not specifically cater to the e-

discovery request. Focusing on the particular data in question is more pertinent.

Option C is incorrect. Deleting potential evidence, especially after a notice for e-discovery, could lead to legal penalties and is not a recommended action.

Option D is incorrect. Informing the media is not a primary step in the e-discovery process and can have detrimental effects on the company's reputation.

Question 528. A cloud-based e-commerce company wants to ensure that its inventory system automatically updates the stock levels on its website and third-party sales platforms whenever a sale occurs. What should the company leverage to achieve this real-time synchronization?

- (A) Regularly backup the inventory system and restore it on the website and sales platforms
- (B) Rely on customers to report discrepancies in stock levels
- (C) **Use Application Programming Interfaces (APIs) to integrate the inventory system with the website and third-party platforms**
- (D) Conduct daily stock audits and manually update all platforms

Explanation 528. Correct Answer: C. Use Application Programming Interfaces (APIs) to integrate the inventory system with the website and third-party platforms. Using APIs ensures real-time data synchronization between systems. Whenever a sale occurs, the inventory system can automatically update stock levels across all platforms.

Option A is incorrect. Backing up and restoring the inventory system is a reactive and inefficient approach. It won't provide real-time stock updates.

Option B is incorrect. Relying on customers to report stock discrepancies is not proactive and could lead to negative customer experiences and potential lost sales.

Option D is incorrect. Manual updates are time-consuming and prone to human error, and they don't support real-time stock level synchronization.

Question 529. A financial organization's high-security data center has an authentication system for its main entry. If the system encounters an unexpected error, the organization wants to ensure that no one can gain access to the data center until the system is fixed. Which configuration should the authentication system be set to?

- (A) Fail-open
- (B) **Fail-closed**
- (C) Fail-secure
- (D) Fail-passive

Explanation 529. Correct Answer: B. Fail-closed. Fail-closed, also known as fail-secure, is a mode where if a system fails, it denies all requests by default, effectively "closing" access. In high-security environments, it's often preferred to prevent any unauthorized access during system failures.

Option A is incorrect. Fail-open is the opposite of what the organization wants. In a fail-open scenario, if the system fails, it would allow all requests by default.

Option C is incorrect. While “fail-secure” is another term for “fail-closed”, the use of both terms in the options can confuse the test-taker. In this context, option B is the more appropriate choice.

Option D is incorrect. Fail-passive isn’t a standard term in the context of authentication failure modes. Fail-open and fail-closed (or fail-secure) are the primary recognized terms.

Question 530. Jane, a security analyst, receives a report about network slowdowns happening at specific times of the day. After investigating, she discovers that a device is flooding the network with traffic, causing legitimate requests to be dropped. Which type of attack is this device likely performing?

- (A) Distributed Denial of Service (DDoS)
- (B) ARP poisoning
- (C) **MAC flooding**
- (D) DNS amplification

Explanation 530. Correct Answer: C. MAC flooding. MAC flooding is an attack that aims to flood the switch’s MAC table with fake MAC addresses until the table overflows. Once it overflows, the switch acts as a hub broadcasting packets to all machines in the network. This can cause significant slowdowns and disruptions.

Option A is incorrect. A Distributed Denial of Service (DDoS) attack uses multiple compromised devices to flood a target with traffic, usually to overwhelm it and take it offline. The scenario describes an internal network slowdown, not an external attack on services.

Option B is incorrect. ARP poisoning is an attack where false ARP messages are sent over a local area network. It's used to link an attacker's MAC address with the IP address of another host. While it can cause disruptions, the primary intent is not to flood the network.

Option D is incorrect. DNS amplification is a type of DDoS attack where an attacker uses publically-accessible DNS servers to flood a target system with DNS response traffic. This does not fit the internal network flooding described in the scenario.

Question 531. A medium-sized financial firm has noticed a series of unauthorized transactions moving funds from legitimate accounts to overseas locations. After investigating, it was found that a group was responsible for exploiting vulnerabilities in the firm's transaction system. Which of the following motivations is most likely driving this group's actions?

- (A) Seeking notoriety within the hacker community
- (B) **Financial gain from unauthorized transactions**
- (C) Demonstrating political beliefs against financial institutions
- (D) Espionage to uncover the firm's investment strategies

Explanation 530. Correct Answer: B. Financial gain from unauthorized transactions. The unauthorized transactions moving funds to overseas locations indicate a direct attempt to illicitly acquire funds, pointing towards a motivation of financial gain.

Option A is incorrect. There's no evidence to suggest the group's actions are driven by a desire for recognition or notoriety. The focus is on moving funds.

Option C is incorrect. While some groups might target financial institutions to make a political statement, the unauthorized transactions to overseas accounts suggest a financial motive, not a political one.

Option D is incorrect. There's no indication the group is interested in the firm's investment strategies. The activity is focused on moving money, not gathering intelligence.

Question 532. Country A and Country B are engaged in an ongoing territorial dispute. Suddenly, critical infrastructure facilities in Country B, such as power plants and transportation hubs, experience systematic cyberattacks. No ransom demand is made, and the attacks lead to significant disruption. What is the most probable motivation behind these cyberattacks?

- (A) Financial gain from market disruptions
- (B) Ethical hackers testing vulnerabilities
- (C) Disruption due to philosophical disagreements with Country B's policies
- (D) Acts of cyberwarfare to weaken Country B's position

Explanation 532. Correct Answer: D. Acts of cyberwarfare to weaken Country B's position. Given the context of the territorial dispute and the specific targeting of critical infrastructures without any ransom demand, it's highly likely that these attacks were intended as acts of cyberwarfare by Country A or its sympathizers to exert pressure on Country B.

Option A is incorrect. While market disruptions can be exploited for financial gains, the context of a territorial dispute and the nature of the attacks suggest a motive tied to geopolitical strategy rather than financial advantage.

Option B is incorrect. Ethical hackers typically identify and report vulnerabilities rather than exploit them to cause widespread disruption.

Option C is incorrect. The attacks were too specific and large-scale to be the work of individuals or groups motivated solely by philosophical disagreements.

Question 533. Alex, an employee at XYZ Corp, noticed an unfamiliar USB drive lying in the company parking lot. Out of curiosity, Alex plugged the device into his workstation. Almost immediately, his antivirus program detected malicious software trying to execute. What type of attack did Alex likely encounter?

- (A) Man-in-the-Middle Attack
- (B) Evil Twin
- (C) Spear Phishing
- (D) **USB Drop Attack**

Explanation 533. Correct Answer: D. USB Drop Attack. A USB Drop Attack involves leaving malware-infected removable devices, such as USB drives, in places where they can be found and used by unsuspecting individuals. Once the device is plugged into a computer, it can potentially execute malicious software or scripts.

Option A is incorrect. A Man-in-the-Middle Attack involves an attacker secretly intercepting and possibly altering the communication between two parties without them noticing. It is not related to USB devices.

Option B is incorrect. Evil Twin refers to a rogue Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications. It doesn't pertain to USB devices.

Option C is incorrect. Spear Phishing is a targeted attempt to steal sensitive information through deceptive emails directed at specific individuals or companies. It is not associated with USB devices.

Question 534. A company is setting up a secure communication channel between its headquarters and a remote branch office. To ensure that data transmitted over this channel originates from a legitimate system at the branch office, the company is considering using digital certificates. Which authentication method for systems is the company contemplating?

- (A) Kerberos authentication
- (B) Password-based authentication
- (C) **Certificate-based authentication**
- (D) Biometric-based authentication

Explanation 534. Correct Answer: C. Certificate-based authentication. Certificate-based authentication uses digital certificates to verify the identity of systems or individuals. In the given scenario, the company wants to verify that data transmitted over the communication channel originates from a legitimate system, making digital certificates an appropriate choice.

Option A is incorrect. Kerberos authentication is a ticket-based authentication protocol primarily used to authenticate users in a network, not specifically for system-to-system authentication using digital certificates.

Option B is incorrect. Password-based authentication requires systems or users to provide a secret password to prove their identity. It doesn't involve the use of digital certificates.

Option D is incorrect. Biometric-based authentication involves using unique physical or behavioral attributes of a person for verification, such as fingerprints or facial patterns. It is not applicable to system-to-system authentication.

Question 535. BioGen Inc., a biotechnology company, has implemented a layered security approach. They are considering adding a human element to their security measures for their research labs. Which of the following would best provide the ability to evaluate and respond to various security situations with human judgment?

- (A) Installing biometric locks
- (B) Employing security guards

- (C) Implementing an access control vestibule
- (D) Deploying AI-driven security cameras

Explanation 535. Correct Answer: B. Employing security guards. Security guards provide the advantage of human judgment and can evaluate, respond, and adapt to a wide variety of security situations, making them ideal for adding a human element to a layered security approach.

Option A is incorrect. While biometric locks can control access based on unique human features, they don't provide the evaluation and response capabilities of a human guard.

Option C is incorrect. An access control vestibule controls access into an area, often with two sets of doors, but it does not provide the evaluation, judgment, or immediate response that a security guard does.

Option D is incorrect. While AI-driven security cameras can provide advanced monitoring and potentially detect suspicious activities, they don't replace the judgment and immediate response capabilities of a human security guard.

Question 536. An environmental NGO's website was hacked and replaced with a message decrying their recent campaign against deforestation, claiming they are spreading misinformation. The website was left with a manifesto promoting responsible forestry and sustainable logging practices. Which type of threat actor is MOST likely behind this incident?

- (A) Ransomware gang

- (B) Organized crime syndicate
- (C) **Hactivist**
- (D) Advanced Persistent Threat (APT)

Explanation 536. Correct Answer: C. Hactivist. The attack seems to be motivated by ideological differences regarding deforestation and sustainable logging. Hacktivists typically conduct cyber actions to make political or social statements. The replacement of the NGO's website with a manifesto supports the idea that this is an ideologically motivated attack, typical of hacktivists.

Option A is incorrect. Ransomware gangs primarily focus on encrypting data and demanding payment for its release. There is no mention of a ransom or encrypted data in the described scenario.

Option B is incorrect. Organized crime syndicates are usually motivated by financial gains. The attack on the NGO's website seems to be ideologically driven, not profit-driven.

Option D is incorrect. Advanced Persistent Threats (APTs) are highly organized, often state-sponsored groups that conduct prolonged cyber-espionage campaigns. Their motivations are typically strategic, political, or espionage-driven. The described attack doesn't fit the profile of an APT operation.

Question 537. After a major data breach in XYZ Corporation, the management decided to understand the primary reason behind the incident to prevent such occurrences in the future. Which of the following approaches should the incident response

team prioritize to determine the fundamental cause of the breach?

- (A) Perform vulnerability scanning on all servers
- (B) Review firewall logs for the past week
- (C) **Conduct a root cause analysis**
- (D) Upgrade all security software

Explanation 537. Correct Answer: C. Conduct a root cause analysis. Root cause analysis (RCA) is a systematic process for identifying the origin of problems or faults and deciding on the most suitable approach to take to prevent recurrence. In the context of a security incident, RCA helps in determining the primary reason behind the breach.

Option A is incorrect. While vulnerability scanning is essential for understanding potential weaknesses in servers, it does not directly identify the fundamental cause of a past incident.

Option B is incorrect. Firewall logs can provide insights about traffic patterns and potential attacks but may not directly reveal the root cause of a breach.

Option D is incorrect. Upgrading security software is a reactive measure and does not ensure understanding or addressing the core reason for a breach.

Question 538. AlphaCorp is migrating to cloud infrastructure and wants to ensure all virtual machines (VMs) are securely configured from the onset. Before deploying multiple VM instances, what should AlphaCorp do to ensure each VM starts from a secure configuration?

- (A) Use the default VM templates provided by the cloud provider
- (B) Establish a secure baseline for VM configurations and use it for deployment**
- (C) Regularly backup all VMs
- (D) Use multi-factor authentication for cloud access

Explanation 538. Correct Answer: B. Establish a secure baseline for VM configurations and use it for deployment.

Establishing a secure baseline for VM configurations ensures that each VM is deployed with a set of standard security settings, reducing vulnerabilities from default configurations or potential misconfigurations.

Option A is incorrect. Relying solely on default VM templates provided by cloud providers may not meet the specific security requirements of an organization. Customizing and creating a secure baseline is more effective.

Option C is incorrect. While regular backups are essential for data recovery, they do not directly ensure that VMs start from a secure configuration.

Option D is incorrect. Multi-factor authentication is a crucial security measure for accessing cloud resources, but it doesn't ensure that VMs are deployed with secure configurations.

Question 539. An employee receives a call from someone claiming to be from the IT department. The caller says there's an urgent update required on the employee's computer and asks for login credentials to perform the update remotely. The

employee becomes suspicious because of which red flag regarding impersonation?

- (A) The caller did not use technical jargon
- (B) **IT normally sends email notifications about updates**
- (C) The employee was not expecting any updates
- (D) The caller's voice sounded unfamiliar

Explanation 539. Correct Answer: B. IT normally sends email notifications about updates. If the organization's standard procedure is to send email notifications about updates, an unsolicited call asking for credentials would be a clear red flag.

Impersonation is a common tactic used in social engineering attacks where the attacker pretends to be someone the victim trusts. Recognizing deviations from standard procedures can help identify impersonation attempts.

Option A is incorrect. The use or lack of technical jargon isn't a reliable indicator of impersonation. Some genuine IT personnel might avoid jargon to make things clearer for non-tech-savvy employees.

Option C is incorrect. While unexpected updates can be suspicious, they aren't necessarily indicative of impersonation on their own. Legitimate unexpected updates can occur.

Option D is incorrect. An unfamiliar voice isn't a reliable indicator since large organizations might have many IT personnel that an employee hasn't interacted with.

Question 540. An organization with a single physical network infrastructure wants to separate the traffic of its finance department from that of the HR department. They do not want to set up entirely new physical networks but want to ensure that data packets from one department do not mix with the other's. What should the organization implement?

- (A) Air-gapped network
- (B) DMZ (Demilitarized Zone)
- (C) **VLAN (Virtual Local Area Network)**
- (D) VPN (Virtual Private Network)

Explanation 540. Correct Answer: C. VLAN (Virtual Local Area Network). A VLAN allows a network administrator to create a logical network within a physical network. This logical segmentation can separate the traffic of different departments, ensuring that data packets from one VLAN do not mix with another, effectively isolating them.

Option A is incorrect. An air-gapped network is a physically isolated network and would require setting up a new physical network.

Option B is incorrect. A DMZ is a buffer zone between a private network and external networks. It doesn't help in segmenting traffic within the internal network.

Option D is incorrect. A VPN is used to create secure connections over an unsecured network. It does not logically segment traffic within a single physical network.

Question 541. After detecting suspicious activity on a network, a digital forensic analyst is dispatched to acquire data from a potential compromised system. The analyst decides to capture an image of the affected system's memory. This technique of capturing volatile data is particularly beneficial because:

- (A) It helps identify deleted files
- (B) **It can capture data in real-time operations**
- (C) It provides information on patch levels
- (D) It offers insights into firewall configurations

Explanation 541. Correct Answer: B. It can capture data in real-time operations. Memory acquisition allows forensic analysts to capture data in its current state, including data about running processes, open network connections, and contents of the system's RAM. This can provide insights into malware or unauthorized activities that occurred in real-time.

Option A is incorrect. While memory acquisition can sometimes provide information about recently accessed files, identifying deleted files is typically done through disk imaging and not memory acquisition.

Option C is incorrect. Information about patch levels is usually gleaned from system configurations and logs, not directly from memory acquisition.

Option D is incorrect. Firewall configurations are typically found in system configurations and logs, not directly from a memory acquisition.

Question 542. A company has faced multiple instances of unauthorized individuals gaining access to their office premises. Which of the following preventive security controls would be MOST effective in preventing unauthorized physical access?

- (A) Implementing a log monitoring solution for network traffic
- (B) Installing video surveillance cameras at all entry and exit points**
- (C) Conducting regular security awareness training for employees
- (D) Implementing a multi-factor authentication system for network access.

Explanation 542. Correct Answer: B. Installing video surveillance cameras at all entry and exit points. Installing video surveillance cameras at all entry and exit points acts as a preventive control by deterring unauthorized individuals from attempting to gain access, given the increased risk of detection and recording.

Option A is incorrect. Implementing a log monitoring solution is a detective control that provides insights into network activities but doesn't prevent unauthorized physical access.

Option C is incorrect. Conducting regular security awareness training is a preventive measure, but its main focus is on making employees aware of security risks and best practices, not directly preventing unauthorized physical access.

Option D is incorrect. Implementing a multi-factor authentication system is a preventive control for unauthorized

digital access but doesn't address the prevention of unauthorized physical access.

Question 543. A software development company is looking to migrate its legacy applications to a more modern infrastructure. They want to ensure the applications can be deployed consistently across multiple environments without the challenges of varying dependencies and configurations. Which approach would best achieve this goal?

- (A) Virtual Machine Deployment
- (B) Bare-Metal Deployment
- (C) **Containerization**
- (D) Serverless Computing

Explanation 543. Correct Answer: C. Containerization

Containerization encapsulates an application and its dependencies into a 'container.' This allows the application to be consistently deployed across different environments regardless of variations in configurations or dependencies.

Option A is incorrect. While virtual machines provide an isolated environment for applications, they include the overhead of an entire guest OS and don't directly address the challenge of application dependencies varying across environments.

Option B is incorrect. Bare-metal deployment involves installing applications directly on hardware without virtualization or containers. This method does not inherently ensure consistent deployment across multiple environments.

Option D is incorrect. Serverless computing abstracts the infrastructure away from the developer, focusing on individual functions. While it provides scalability and simplicity, it doesn't directly address consistent deployment across environments due to dependencies and configurations.

Question 544. While conducting a security assessment, Lucy found that a specific application crashes when she inputs a string that is much longer than what the input field is designed to handle. This could potentially allow her to execute arbitrary code in the application's context. What vulnerability is Lucy likely trying to exploit?

- (A) SQL Injection
- (B) Cross-Site Scripting (XSS)
- (C) **Buffer Overflow**
- (D) Directory Traversal

Explanation 544. Correct Answer: C. Buffer Overflow.

Buffer overflow vulnerabilities occur when data written to a buffer exceeds that buffer's boundaries, potentially overwriting adjacent memory locations. If exploited successfully, it can lead to arbitrary code execution.

Buffer overflow is a condition where an application writes more data to a buffer than it can hold, causing the excess data to overflow into adjacent memory spaces. When this happens, attackers can overwrite specific parts of the memory, which may lead to arbitrary code execution, application crashes, or data corruption.

Option A is incorrect. SQL Injection involves injecting malicious SQL statements into an entry field for execution, aiming to manipulate a database. It doesn't relate to buffer boundaries or memory overflows.

Option B is incorrect. Cross-Site Scripting (XSS) allows attackers to inject malicious scripts into web pages viewed by other users. While this is an input validation flaw like a buffer overflow, XSS specifically targets script execution within web browsers and does not involve overflowing buffer boundaries.

Option D is incorrect. Directory Traversal attacks aim to access files and directories stored outside the web root folder. They don't involve overflowing buffer boundaries or memory overflows.

Question 545. A major pharmaceutical company recently announced an increase in drug prices. Following the announcement, their website was taken offline by a DDoS attack, with a message posted online by a group claiming responsibility and demanding affordable healthcare for all. Which type of threat actor is MOST likely behind this attack?

- (A) Unskilled attacker
- (B) Insider threat
- (C) **Hacktivist**
- (D) Nation-state

Explanation 545. Correct Answer: C. Hacktivist. Hacktivists are typically driven by political, social, or ideological motives. They use cyber attacks as a means to promote or protest certain issues. In this scenario, the attack on the pharmaceutical

company is a form of protest against their pricing policies, making it characteristic of hacktivist behavior.

Option A is incorrect. Unskilled attackers generally conduct attacks for personal bragging rights or mischief. They are not usually driven by ideological motives like demanding affordable healthcare.

Option B is incorrect. Insider threats stem from individuals within the organization, often driven by personal grievances or financial gain. The described scenario shows a motive tied to a broader social issue, not a personal or internal motive.

Option D is incorrect. Nation-states conduct cyber operations for political, espionage, or military reasons. Protesting drug prices is not in line with their typical objectives.

Question 546. After a security breach, Jake, a digital forensics investigator, arrives at the scene to collect a hard drive for examination. He labels the hard drive, records its serial number, photographs the scene, and ensures the hard drive is transported securely to the forensics lab. These steps are crucial to:

- (A) Preserve the data's integrity on the hard drive
- (B) **Maintain the chain of custody**
- (C) Decrypt the data on the hard drive
- (D) Implement a legal hold on the data

Explanation 546. Correct Answer: B. Maintain the chain of custody. Maintaining a chain of custody is crucial to ensure that evidence is authentic and unchanged. This involves

documenting each step of the evidence handling process, from collection to analysis, ensuring its validity in legal proceedings.

Option A is incorrect. While preserving the data's integrity is crucial in forensics, the specific steps mentioned are primarily for maintaining the chain of custody.

Option C is incorrect. Decrypting the data focuses on making encrypted data readable. The steps Jake took are related to documenting evidence handling, not decryption.

Option D is incorrect. Implementing a legal hold ensures that specific data is preserved for legal reasons. The steps mentioned by Jake focus on documenting how the evidence was handled and preserved, not on a directive to retain it for legal purposes.

Question 547. A security analyst has been tasked with investigating a possible data breach. While reviewing the network logs, the analyst noticed an unusual increase in outbound traffic to an unfamiliar IP address during non-business hours. The traffic appears to be encrypted and is associated with a known server containing sensitive data. Which of the following is the MOST likely explanation for this behavior?

- (A) The server is downloading patches
- (B) An employee is accessing the server remotely
- (C) A backup of the server is being performed
- (D) **Data exfiltration is occurring**

Explanation 547. Correct Answer: D. Data exfiltration is occurring. Given that the traffic is encrypted, associated with a sensitive server, and is being sent to an unfamiliar IP during

non-business hours, the most likely scenario is that unauthorized data is being taken out of the network, which is known as data exfiltration.

Option A is incorrect. While servers do download patches, these are usually inbound traffic from a known update source, not outbound to unfamiliar IPs.

Option B is incorrect. While employees might access servers remotely, the traffic being encrypted and sent during non-business hours to an unfamiliar IP makes this less likely.

Option C is incorrect. Backups generally don't result in encrypted outbound traffic to unfamiliar IP addresses, especially during non-business hours.

Question 548. XYZ Corporation recently faced a major power outage that affected their primary data center. During the incident, it was found that there was no clear guidance on the steps to maintain or quickly restore business operations. To address this, which of the following policies should XYZ Corporation prioritize implementing?

- (A) Data Classification Policy
- (B) **Business Continuity Policy**
- (C) Acceptable Use Policy
- (D) Network Segmentation Strategy

Explanation 548. Correct Answer: B. Business Continuity Policy. A Business Continuity Policy outlines the processes and procedures an organization should follow to ensure that essential functions can continue during and after a disaster. It

provides a roadmap for maintaining and quickly restoring business operations.

Option A is incorrect. The Data Classification Policy is concerned with categorizing data based on its sensitivity but doesn't address continuity of business operations during disruptions.

Option C is incorrect. The Acceptable Use Policy specifies how the organization's IT resources and networks can be used by employees. It doesn't provide guidance on restoring business operations during a disaster.

Option D is incorrect. While Network Segmentation Strategy is crucial for security, dividing the network into segments does not specifically address business continuity during major disruptions.

Question 549. During a suspected security incident involving unauthorized access to sensitive data, Jake, an IT administrator, immediately disconnected the affected server from the network. Later, a digital forensic expert criticized Jake's action. Which of the following is the MOST likely reason for the criticism?

- (A) Jake should have left the server connected to capture more evidence from the attacker
- (B) Jake should have immediately informed the company's legal department
- (C) **Jake should have taken an image of the server's memory before disconnecting it**
- (D) Jake should have updated the server's software to prevent further unauthorized access

Explanation 549. Correct Answer: C. Jake should have taken an image of the server's memory before disconnecting it. Preserving the current state of a system, especially its volatile memory, is crucial during a digital forensic investigation. Volatile memory can contain critical evidence about an incident, but this evidence is lost once the system is powered off or restarted.

Option A is incorrect. While sometimes monitoring an attacker can be valuable, it's often more critical to prioritize the safety of data and systems over collecting additional evidence.

Option B is incorrect. Although informing the legal department is an important step in many incident response processes, preserving the integrity and state of potential evidence comes first.

Option D is incorrect. While updating the server's software might be a future step to prevent incidents, the immediate priority during a suspected security incident is to preserve evidence.

Question 550. ExamsDigest Corp, a technology company, recently conducted a security assessment to align with industry best practices. The company's current security posture was compared to its desired future state, revealing discrepancies. Which of the following best describes the approach ExamsDigest Corp employed?

- (A) Vulnerability Assessment
- (B) Penetration Testing

- (C) Gap Analysis
- (D) Threat Modeling

Explanation 550. Correct Answer: C. Gap Analysis. Gap analysis is a method of comparing the current state of something (such as security measures) with a future desired state to identify the discrepancies or “gaps”. In the scenario, ExamsDigest Corp compared their current security posture to a desired future state, which is consistent with the process of gap analysis.

Option A is incorrect. A vulnerability assessment focuses on identifying, quantifying, and ranking vulnerabilities in a system, not comparing the current state with a desired future state.

Option B is incorrect. Penetration testing is an authorized simulated cyberattack on a system to evaluate its security, not to compare its current state with a desired future state.

Option D is incorrect. Threat modeling is the process of identifying potential threats to a system and determining the risk they pose, not comparing the current state with a desired future state.

Question 551. During an annual review, a company discovered that one of its critical systems had several unscheduled downtimes over the year. The CTO has recommended a move towards high availability architecture to address this. What is the PRIMARY concern when implementing high availability?

- (A) Ensuring that there are no single points of failure
- (B) Ensuring that the system is patched regularly

- (C) Implementing multi-factor authentication
- (D) Storing backups in multiple geographical locations

Explanation 551. Correct Answer: A. Ensuring that there are no single points of failure. In a high availability (HA) system, eliminating single points of failure is of utmost importance. By ensuring redundancy at every potential failure point, the system can remain operational even if a component fails.

Option B is incorrect. While patching is important for security, it is not the primary concern when implementing high availability.

Option C is incorrect. Multi-factor authentication is essential for secure access but does not directly relate to high availability architecture.

Option D is incorrect. Having backups in various geographical locations is more relevant to disaster recovery than to high availability.

Question 552. A government agency experienced a cyber incident where its communication platforms were breached. The intruders were not interested in extracting sensitive data or causing disruptions but were observed to be silently monitoring diplomatic communications for an extended period. What was the likely motivation of the attackers?

- (A) To gain financial benefits from insider trading
- (B) **Espionage to understand and anticipate diplomatic moves**

- (C) Disgruntlement of an internal employee
- (D) An attempt to expand their cybercriminal network

Explanation 552. Correct Answer: B. Espionage to understand and anticipate diplomatic moves. Silently monitoring diplomatic communications without exfiltrating data or causing disruptions indicates a motivation to understand, anticipate, and potentially manipulate governmental or diplomatic actions. This is a classic example of espionage.

Option A is incorrect. While sensitive information might indeed be valuable for insider trading, the focus on diplomatic communications suggests a broader strategic intent rather than just financial gain.

Option C is incorrect. A disgruntled employee might engage in sabotage or data leakage, but silently monitoring diplomatic communications indicates a higher level of strategy and sophistication usually beyond personal vendettas.

Option D is incorrect. The attackers' actions were specific to monitoring diplomatic channels and did not indicate an attempt to recruit more systems or individuals into a criminal network.

Question 553. AlphaTech's IT department is rolling out a new authentication protocol for remote workers. As part of the multifactor authentication process, employees are required to provide information that is memorized and cannot be physically taken from them. Which of the following represents this type of authentication factor?

- (A) Fingerprint

- (B) Smart card
- (C) PIN
- (D) USB security key

Explanation 553. Correct Answer: C. PIN. A Personal Identification Number (PIN) represents the “something you know” factor in multifactor authentication. This type of information is memorized by the user and is not a physical item that can be taken or a biological trait.

Option A is incorrect. A fingerprint represents the “something you are” factor, which pertains to biometrics.

Option B is incorrect. A smart card represents the “something you have” factor, as it’s a physical item that a user possesses.

Option D is incorrect. A USB security key also falls under the “something you have” factor. It’s a physical device rather than memorized information.

Question 554. An IT department in a large corporation spends several hours each day manually deploying patches and updates to thousands of workstations. Which of the following solutions would BEST enhance the efficiency of this process and save time for the IT team?

- (A) Disable automatic updates and conduct monthly patching sessions
- (B) **Implement an automated patch management system**
- (C) Designate a dedicated team for patching that operates in shifts
- (D) Educate users to install updates on their own

Explanation 554. Correct Answer: B. Implement an automated patch management system. By implementing an automated patch management system, the IT department can streamline the deployment of patches and updates across all workstations, ensuring consistency, reducing manual efforts, and saving valuable time.

Option A is incorrect. Disabling automatic updates and conducting monthly patching sessions does not address the inefficiency of manual patching and might expose the systems to vulnerabilities for a longer time.

Option C is incorrect. While designating a dedicated team might distribute the workload, it doesn't eliminate the inefficiencies associated with manual patching.

Option D is incorrect. Relying on users to install updates introduces inconsistency, potential delays, and additional risks, as not all users might have the technical knowledge or remember to update regularly.

Question 555. A large e-commerce platform is facing challenges during peak sale periods, where the influx of users causes slowdowns and occasional outages. Which of the following solutions would BEST improve scalability during these high-demand times?

- (A) Implement a centralized logging system
- (B) **Employ auto-scaling cloud solutions**
- (C) Increase the frequency of data backups
- (D) Mandate regular security training for employees

Explanation 555. Correct Answer: B. Employ auto-scaling cloud solutions. Auto-scaling in cloud solutions automatically adjusts the number of computational resources based on the actual demand. During peak periods, resources can be automatically increased to handle the demand, ensuring the system remains scalable and responsive.

Option A is incorrect. A centralized logging system is beneficial for monitoring and troubleshooting, but it does not directly address scalability during peak times.

Option C is incorrect. Increasing the frequency of data backups is a good practice for data integrity and recovery but does not handle scalability concerns directly.

Option D is incorrect. Regular security training is crucial for a company's cybersecurity posture, but it does not address the architectural scalability of the platform.

Question 556. Alex, a new intern at an IT company, wanted to access the internal company portal. Instead of typing "companyportal.com," he accidentally typed "comapnyportal.com" and ended up on a site that looked identical but asked him to download a security certificate. This scenario best describes which type of attack?

- (A) Spear Phishing
- (B) Watering Hole Attack
- (C) **Typosquatting**
- (D) Man-in-the-Middle

Explanation 556. Correct Answer: C. Typosquatting. The attacker relies on typographical errors made by users when inputting a URL into a web browser, then potentially tries to exploit the user in some manner on the deceptive site.

Typosquatting, also known as URL hijacking, involves attackers registering domains that are misspellings of popular websites. The intent is often to deceive users who mistype a URL, leading them to malicious websites.

Option A is incorrect. Spear Phishing targets specific individuals or companies with tailored attempts to steal information. The described scenario revolves around the exploitation of typographical errors, not a targeted email attack.

Option B is incorrect. A Watering Hole Attack involves compromising a specific website or service that the target frequently uses. It doesn't rely on typographical errors.

Option D is incorrect. A Man-in-the-Middle attack involves an attacker secretly intercepting and potentially altering communication between two parties. This is not described in the scenario.

Question 557. A cloud infrastructure team frequently receives performance alerts from various resources in the environment. They want to ensure that relevant teams are immediately informed and can act upon any resource that crosses a performance threshold. What is the BEST way to accomplish this?

(A) Conduct a weekly meeting to review all performance

alerts

(B) Automate ticket creation for any resource that crosses the performance threshold and assign it to the relevant team

(C) Send all performance alerts to the cloud infrastructure team's email for review

(D) Disable performance monitoring to reduce alert fatigue

Explanation 557. Correct Answer: B. Automate ticket creation for any resource that crosses the performance threshold and assign it to the relevant team. Automating the ticket creation process ensures that alerts are not overlooked and that the appropriate teams are informed in real-time, allowing for prompt resolution.

Option A is incorrect. Conducting a weekly review does not allow for immediate action upon critical performance issues.

Option C is incorrect. Sending all alerts to the team's email might lead to alert fatigue and the possibility of overlooking critical alerts among less important ones.

Option D is incorrect. Disabling performance monitoring would prevent the team from receiving important alerts and is not a practical solution.

Question 558. A large corporation is investigating a potential insider threat incident. A security analyst is tasked with examining the OS-specific security logs of a Windows server where sensitive documents are stored. Which of the following entries in the logs would MOST likely indicate unauthorized

access attempts?

- (A) Logs displaying Windows Update successful installations
- (B) Entries showing a large number of failed login attempts followed by a successful login from a user outside of regular business hours**
- (C) Logs indicating scheduled disk defragmentation tasks
- (D) Entries detailing successful printer connections and print jobs

Explanation 558. Correct Answer: B. Entries showing a large number of failed login attempts followed by a successful login from a user outside of regular business hours. A sequence of failed login attempts followed by a successful login, especially outside of regular business hours, can be a strong indicator of a brute-force attack or unauthorized access attempt on a system.

Option A is incorrect. Successful installations of Windows Updates are routine maintenance activities and do not directly imply unauthorized access.

Option C is incorrect. Disk defragmentation tasks are part of regular system maintenance and are not indicative of unauthorized access.

Option D is incorrect. While monitoring printer connections and print jobs can be relevant in certain security investigations, they are not direct indicators of unauthorized server access.

Question 559. A company wants to ensure that security incidents are detected and addressed as quickly as possible by on-duty personnel. Which of the following operational security controls would be BEST to implement for this purpose?

- (A) Deploying a Network Intrusion Prevention System (NIPS)
- (B) Establishing a 24/7 Security Operations Center (SOC)
- (C) Creating a company-wide security policy
- (D) Implementing end-to-end data encryption

Explanation 559. Correct Answer: B. Establishing a 24/7 Security Operations Center (SOC). A Security Operations Center (SOC) is an operational control that provides real-time monitoring, detection, and response to security incidents. With a 24/7 SOC, the company ensures that there is always personnel available to handle security incidents as they occur.

Option A is incorrect. Deploying a Network Intrusion Prevention System (NIPS) is a technical control. While it can prevent unauthorized activities on the network, it does not ensure that there is personnel available around the clock to address incidents.

Option C is incorrect. Creating a company-wide security policy is a managerial control. It sets the guidelines and procedures for security but does not ensure continuous monitoring and immediate response to incidents.

Option D is incorrect. Implementing end-to-end data encryption is a technical control that ensures data

confidentiality. While it protects data, it does not ensure that incidents are detected and addressed by on-duty personnel in real-time.

Question 560. AlphaCorp's IT department is reviewing password policies and wants to adopt a strategy that enhances security. Which of the following password strategies would be the MOST secure?

- (A) Passwords should be at least 6 characters long, with no other requirements
- (B) Passwords should be at least 10 characters long and include both uppercase and lowercase letters
- (C) **Passwords should be at least 8 characters long and include uppercase letters, lowercase letters, numbers, and special characters**
- (D) Passwords should be at least 4 characters long and include a mix of uppercase and lowercase letters

Explanation 560. Correct Answer: C. Passwords should be at least 8 characters long and include uppercase letters, lowercase letters, numbers, and special characters. This option provides a balanced combination of length and complexity, making it more resistant to brute-force and dictionary attacks.

Option A is incorrect. A 6-character password without any complexity requirements is easier to crack with modern computational capabilities.

Option B is incorrect. While having a 10-character length is beneficial, it lacks the additional complexity of numbers and special characters which can further bolster security.

Option D is incorrect. The length is too short, and even with a mix of uppercase and lowercase, it does not provide the recommended security for passwords.

Question 561. SecureTech Corp, a company dealing with sensitive client data, is redesigning its main office entrance to enhance security. They want to ensure that only one person gains access at a time, even if multiple people try to enter using a single authorized access badge. Which of the following would best serve this purpose?

- (A) CCTV Cameras
- (B) **Mantrap**
- (C) Biometric Scanners
- (D) Motion Detectors

Explanation 561. Correct Answer: B. Mantrap. A mantrap, also known as an access control vestibule, is a physical security access control system comprising a small space with two sets of interlocking doors. The first door must close before the second door opens, ensuring that only one person can pass through at a time. This design prevents tailgating or piggybacking, where unauthorized individuals attempt to enter a secure area by following closely behind an authorized individual.

Option A is incorrect. While CCTV cameras monitor and record activities, they do not physically prevent multiple people from entering at once using a single access badge.

Option C is incorrect. Biometric scanners provide a means of authenticating individuals based on unique physical or behavioral characteristics, but they do not prevent tailgating on their own.

Option D is incorrect. Motion detectors can detect movement but do not restrict the entry of multiple individuals trying to use a single authorized access badge.

Question 562. After a recent incident of vandalism, a corporate building is considering implementing security controls that would dissuade potential perpetrators. Which of the following would serve BEST as a deterrent control?

- (A) Encrypting all stored data
- (B) Installing biometric access controls on all entrances
- (C) Implementing regular data backups
- (D) **Placing visible security signage indicating 24/7 surveillance**

Explanation 562. Correct Answer: D. Placing visible security signage indicating 24/7 surveillance. Visible security signage serves as a deterrent control as it discourages potential perpetrators by signaling the risk of detection and consequences, even if actual surveillance might not be active at all times.

Option A is incorrect. Encrypting all stored data is a preventive control that ensures unauthorized individuals cannot access or understand the encrypted information. It doesn't deter acts of physical vandalism.

Option B is incorrect. Installing biometric access controls is a preventive control that restricts physical access based on unique biological attributes. While it prevents unauthorized access, it doesn't act as a visible deterrent to vandalism or other potential threats.

Option C is incorrect. Implementing regular data backups is a corrective control designed to restore data after a security incident. It doesn't deter potential threats.

Question 563. After deploying a new version of your company's internal application, several users reported issues with accessing specific features. To investigate the root cause, you decided to review the application logs. What entry in the logs would most directly indicate a software bug or error related to the recent deployment?

- (A) Entries showing successful user authentication timestamps
- (B) Entries detailing the number of transactions completed by the application
- (C) **Entries with "ERROR" or "EXCEPTION" related to the specific feature being accessed**
- (D) Entries showing routine data backup operations

Explanation 563. Correct Answer: C. Entries with "ERROR" or "EXCEPTION" related to the specific feature being accessed. In the context of application logs, entries labeled as "ERROR" or "EXCEPTION" generally indicate that the application encountered a problem. If these entries are related to the feature users are having trouble with, it points towards a software bug or issue related to the deployment.

Option A is incorrect. Successful user authentication entries would indicate that users are able to log into the application successfully, but they don't provide insights into feature-specific issues.

Option B is incorrect. While the number of transactions could provide performance metrics or usage patterns, it doesn't directly indicate a software bug or deployment-related issue.

Option D is incorrect. Routine data backup operations are unrelated to application feature functionalities and won't help in identifying deployment-related errors.

Question 564. OmegaTech recently introduced an additional layer of security for its remote server access. Along with their usual passwords, employees now need to use a physical device they have with them to gain access. Which of the following represents this “something you have” factor in multifactor authentication?

- (A) Password hint
- (B) Facial recognition
- (C) **Hardware token**
- (D) Voice recognition

Explanation 564. Correct Answer: C. Hardware token.

Hardware tokens are devices that generate security codes for authentication purposes. Users are required to have this physical device on-hand, making it an example of the “something you have” factor in multifactor authentication.

Option A is incorrect. A password hint is related to “something you know” factor. Moreover, it’s not an authentication factor but rather an aid for recalling a password.

Option B is incorrect. Facial recognition pertains to the “something you are” factor, which refers to biometric methods of authentication.

Option D is incorrect. Voice recognition, similar to facial recognition, falls under the “something you are” factor, as it uses biometric identification.

Question 565. A system administrator is setting up an authentication system for a new web application. Which of the following security controls falls under the technical category and ensures that users prove their identity before gaining access?

- (A) Implementing a security awareness training program
- (B) Conducting a background check for new employees
- (C) **Using multi-factor authentication**
- (D) Establishing a clean desk policy

Explanation 565. Correct Answer: C. Using multi-factor authentication. Multi-factor authentication is a technical control that requires users to present two or more pieces of evidence (factors) before gaining access. It provides an additional layer of security to ensure that users are who they say they are.

Option A is incorrect. Implementing a security awareness training program is an administrative control, as it involves

educating employees on security best practices rather than using technical measures to enforce them.

Option B is incorrect. Conducting a background check is an administrative control as it involves vetting potential employees before they're hired. This process doesn't directly enforce technical measures on systems or networks.

Option D is incorrect. Establishing a clean desk policy is an administrative control. It sets a guideline for employees to keep their workspaces tidy and free of sensitive information, rather than enforcing technical measures.

Question 566. BetaTech is implementing a new authentication mechanism for its data center technicians. Instead of using key cards, technicians will now have to look into a device that maps a specific pattern to authenticate their identity. Which of the following is BetaTech likely implementing?

- (A) Password system
- (B) **Retina scanning**
- (C) Hardware token
- (D) Knowledge-based questions

Explanation 566. Correct Answer: B. Retina scanning.

Retina scanning is a biometric method that analyzes the unique patterns of a person's retina to authenticate their identity. It's categorized under the "something you are" factor as it relies on a unique physical characteristic.

Option A is incorrect. A password system pertains to the “something you know” factor since users need to remember their passwords to authenticate.

Option C is incorrect. A hardware token represents the “something you have” factor, as it’s a device the user needs to possess.

Option D is incorrect. Knowledge-based questions, such as “What’s the name of your first pet?”, fall under the “something you know” factor.

Question 567. DataCenter Inc. is located in a region prone to protests and vandalism. They wish to enhance their perimeter security to deter potential intruders and make it visibly clear that unauthorized access is restricted. Which of the following physical security measures would be the most effective first line of defense for the company?

- (A) Sliding Doors
- (B) Security Cameras
- (C) **High-security Fencing**
- (D) Proximity Card Readers

Explanation 567. Correct Answer: C. High-security Fencing.

High-security fencing is a primary physical barrier that serves to deter, delay, and detect intrusions. It provides a clear visual indicator that delineates private property and can be equipped with additional deterrents such as barbed wire or sensors. Especially in areas prone to vandalism or protests, a robust fence acts as an immediate barrier to unauthorized access.

Option A is incorrect. Sliding doors are more applicable to internal security or entrance points and do not serve as a primary external barrier.

Option B is incorrect. While security cameras monitor and record activities, they do not serve as a physical barrier to prevent or deter unauthorized access.

Option D is incorrect. Proximity card readers are a form of access control that checks the credentials of individuals but do not serve as a primary deterrent against vandalism or protests.

Question 568. Alice wants to access a restricted online portal. The portal asks her to enter a unique username and a secret passphrase only she should know. This process helps the system ensure that Alice is who she claims to be. What security concept is the portal employing?

- (A) Authorization
- (B) Accounting
- (C) Multifactor authentication
- (D) **Authentication**

Explanation 568. Correct Answer: D. Authentication.

Authentication is the process of verifying the identity of a user, system, or application. In the described scenario, Alice is proving her identity to the system by providing a unique username and a passphrase, which are credentials that supposedly only she possesses.

Option A is incorrect. Authorization determines what actions, resources, or services a verified identity is allowed to access or perform. It does not deal with verifying the identity itself.

Option B is incorrect. Accounting involves tracking user activities and recording them for audit purposes. It does not directly verify a user's identity.

Option C is incorrect. Multifactor authentication requires two or more methods of verification from different categories of credentials. The scenario only mentioned a username and passphrase, which is a single-factor authentication method.

Question 569. Employees at a renowned software development firm frequently visit an industry-related forum to discuss the latest trends and technologies. Over the past month, several employees reported malware infections shortly after accessing the forum. An investigation suggests the forum was compromised to target the company's developers specifically. Which type of attack most accurately describes this scenario?

- (A) Spear Phishing
- (B) **Watering Hole**
- (C) Drive-by Download
- (D) Whaling

Explanation 569. Correct Answer: B. Watering Hole. The attack focused on a particular site that employees at the targeted organization are known to visit, intending to compromise those specific individuals.

A watering hole attack involves compromising a website or online resource frequented by members of a particular group or organization. Once compromised, attackers can use the site to deploy malware to the targeted individuals.

Option A is incorrect. Spear phishing is a targeted phishing attempt, typically via email, aimed at a specific individual or organization. It does not involve compromising websites that targets frequent.

Option C is incorrect. While a drive-by download might be the method used to deliver malware once the forum was compromised, the overall strategy of targeting a specific site known to be frequented by the victims defines it as a watering hole attack.

Option D is incorrect. Whaling is a type of phishing attack aimed at high-profile targets like CEOs or CFOs. It doesn't involve compromising websites.

Question 570. A cybersecurity analyst at XYZ Corp is looking to deploy a system that appears to be vulnerable and enticing to attackers. The main goal is to study the tactics, techniques, and procedures (TTPs) of potential adversaries, without them realizing that they're interacting with a decoy. Which of the following would BEST meet this requirement?

- (A) Intrusion Detection System (IDS)
- (B) Firewall
- (C) **Honeypot**
- (D) VPN Concentrator

Explanation 570. Correct Answer: C. Honeypot. A honeypot is a security mechanism designed to lure attackers into interacting with a seemingly vulnerable system. Its primary purpose is not to block or prevent attacks but to log and study them. By analyzing the activities on the honeypot, security professionals can gain insights into the methods and motivations of the attackers.

Option A is incorrect. An Intrusion Detection System (IDS) is designed to detect malicious activities on a network and alert administrators. While it can identify threats, it doesn't actively lure attackers.

Option B is incorrect. A firewall is designed to block or allow traffic based on specific rules. It doesn't present itself as a vulnerable target to lure attackers.

Option D is incorrect. A VPN Concentrator is a device that provides remote access to a network over a secure connection. Its primary purpose is to enable secure remote access, not to act as a decoy for attackers.

Question 571. A large financial organization wants to ensure that all employees understand the importance of cybersecurity and the role they play in safeguarding company assets. Which of the following managerial security controls will be MOST effective in achieving this?

- (A) Installing a firewall at the network perimeter
- (B) **Regular security awareness training for employees**
- (C) Deploying an Intrusion Detection System (IDS)
- (D) Encrypting all company data

Explanation 571. Correct Answer: B. Regular security awareness training for employees. Security awareness training is a managerial control aiming to educate employees about security risks and the necessary precautions they need to take. By regularly training employees, the organization ensures that all staff are aware of potential threats and their roles in cybersecurity.

Option A is incorrect. Installing a firewall is a technical control focused on preventing unauthorized access to or from a private network. While it protects the network, it doesn't directly educate employees about their roles in cybersecurity.

Option C is incorrect. Deploying an Intrusion Detection System (IDS) is a technical control. It monitors network traffic for suspicious activities but does not directly focus on educating employees.

Option D is incorrect. Encrypting company data is a technical control. While it ensures the confidentiality of data, it doesn't address the employees' knowledge or awareness regarding cybersecurity.

Question 572. You are an IT security professional for a large corporation. After receiving reports about some users being unable to access external websites, you decided to review the firewall logs. Which of the following would be a PRIMARY indicator in the logs that a rule is blocking outbound traffic?

- (A) Multiple entries of the same external IP address being ALLOWED
- (B) Timestamps showing large gaps between entries

(C) Entries showing DROP/REJECT action for outbound traffic to port 80 and 443

(D) Logs showing inbound traffic from multiple unknown external IP addresses

Explanation 572. Correct Answer: C. Entries showing DROP/REJECT action for outbound traffic to port 80 and 443. Port 80 and 443 are standard ports for HTTP and HTTPS respectively, which are commonly used for accessing websites. If users are unable to access external websites, it would make sense to check for DROP or REJECT actions for these ports in the firewall logs.

Option A is incorrect. If an external IP address is being ALLOWED multiple times, it wouldn't be the cause of users being unable to access websites.

Option B is incorrect. Large gaps between timestamps in logs can indicate various issues, but they aren't a direct indicator of a specific rule blocking outbound traffic.

Option D is incorrect. While inbound traffic from unknown IP addresses might be of concern, it doesn't specifically indicate an outbound traffic rule blocking users from accessing websites

Question 573. A digital forensics investigator has just concluded an investigation regarding a potential insider threat. Before presenting the findings to the organization's board, which of the following should the investigator ensure about the forensic report?

(A) The report includes technical jargon to showcase the

depth of the investigation

(B) The report emphasizes the investigator's credentials and experience

(C) **The report provides a clear, concise summary of findings without unnecessary technical details**

(D) The report contains detailed logs of every action taken by the investigator

Explanation 573. Correct Answer: C. The report provides a clear, concise summary of findings without unnecessary technical details. A forensic report's primary purpose is to convey the results of an investigation in a clear and understandable manner, especially to non-technical stakeholders. By avoiding unnecessary technical jargon and providing a concise summary, it ensures that the report's findings are accessible to all intended readers.

Option A is incorrect. While the depth of an investigation is important, inundating a report with technical jargon can make it difficult for non-technical individuals, such as board members, to understand the findings.

Option B is incorrect. While the investigator's credentials and experience might be important, they should not be the emphasis of the report. The focus should remain on the investigation's findings and their implications.

Option D is incorrect. While maintaining a detailed log of every action taken is crucial for the investigator's records and ensuring the integrity of the investigation, including every detail

in the report can be overwhelming and detract from its main findings.

Question 574. The security team at WidgetCorp is trying to identify potential insider threats. They have set up a SIEM solution with a custom dashboard showing unusual activities. Which of the following dashboard views would be MOST effective for quickly identifying an employee uploading large amounts of proprietary data to an external cloud storage service?

- (A) Display of users who logged in during off-hours
- (B) **Graph of highest network bandwidth users**
- (C) List of most frequently used applications
- (D) Visualization of failed login attempts

Explanation 574. Correct Answer: B. Graph of highest network bandwidth users. When an employee uploads large amounts of data to an external service, it typically results in a significant spike in network bandwidth. Therefore, a dashboard view that visually displays the highest network bandwidth users can quickly alert the security team to potential data exfiltration activities.

Option A is incorrect. While logging in during off-hours can be suspicious, it doesn't directly correlate to data upload activities.

Option C is incorrect. A list of the most frequently used applications might help in determining the common tools used within the organization, but it doesn't specifically point to data upload actions.

Option D is incorrect. Visualization of failed login attempts could show potential brute-force or unauthorized access attempts, but it doesn't directly indicate data uploading activities.

Question 575. During a regular review of system logs, Alex, a security analyst, noticed an unusual pattern of network traffic originating from a single IP address. Instead of waiting for an automated system to flag this as suspicious, he decides to manually dive deeper into the data to identify any potential threats. What is Alex engaging in?

- (A) Incident management
- (B) Threat modeling
- (C) **Threat hunting**
- (D) Security monitoring

Explanation 575. Correct Answer: C. Threat hunting. Threat hunting is a proactive approach where security professionals or analysts actively and manually search for signs of malicious activities within their network or systems, especially those threats that haven't been automatically detected by traditional security tools.

Option A is incorrect. Incident management refers to the process followed when managing and responding to a security incident. In this scenario, Alex is taking a proactive approach to find potential threats, not responding to an identified incident.

Option B is incorrect. Threat modeling involves identifying potential threats and designing countermeasures to prevent or

mitigate the impact of those threats. It's more about planning than actively searching for threats.

Option D is incorrect. Security monitoring is the process of continuously monitoring and analyzing an organization's security events. While Alex is reviewing logs, which is part of monitoring, the manual and proactive deep dive he is taking is more in line with threat hunting.

Question 576. OmegaTech's security team noticed an increase in account compromises. An internal investigation revealed that many employees have been using the same passwords across different company systems and applications. Which password best practice can OmegaTech enforce to mitigate this issue?

- (A) Encouraging users to change their passwords every month
- (B) Implementing an account lockout policy after three failed login attempts
- (C) **Prohibiting password reuse for at least the last five password changes**
- (D) Mandating that passwords contain only alphabetical characters for simplicity

Explanation 576. Correct Answer: C. Prohibiting password reuse for at least the last five password changes. By prohibiting password reuse for a number of iterations, you discourage users from cycling between a small set of passwords and, therefore, increase the overall security of user accounts.

Option A is incorrect. While frequent password changes can enhance security, they don't directly address the issue of password reuse across different systems and applications.

Option B is incorrect. While an account lockout policy can deter brute-force attacks, it doesn't prevent users from reusing the same passwords across different platforms.

Option D is incorrect. Restricting passwords to only alphabetical characters reduces complexity and weakens the security of the password.

Question 577. A medium-sized company suffered a data breach. Investigations revealed that an attacker from a rival firm had exploited a misconfigured firewall to gain unauthorized access to the company's database. Based on the attributes of the actor, how would this threat actor be best described?

- (A) Internal actor leveraging physical access
- (B) Internal actor abusing privileges
- (C) External actor using social engineering
- (D) **External actor exploiting technical vulnerabilities**

Explanation 577. Correct Answer: D. External actor exploiting technical vulnerabilities. The attacker originated from outside the victim organization (a rival firm) and exploited a technical issue (misconfigured firewall) to gain access. This categorizes them as an external actor exploiting technical vulnerabilities.

Option A is incorrect. The attacker was from a rival firm and did not utilize physical access within the victim organization. Therefore, this description doesn't match the scenario.

Option B is incorrect. The scenario doesn't mention any internal actors or abuse of privileges. Instead, it describes an external attacker from a rival firm.

Option C is incorrect. While the attacker was external, the scenario does not describe any use of social engineering tactics. Instead, the attacker exploited a technical vulnerability (misconfigured firewall).

Question 578. In a microservices architecture, each service should be designed with a specific principle to ensure it performs a specific task and interacts with other services through well-defined interfaces. What principle is this referring to?

- (A) Principle of Least Privilege
- (B) **Single Responsibility Principle**
- (C) Open-Closed Principle
- (D) Zero Trust Model

Explanation 578. Correct Answer: B. Single Responsibility Principle. The Single Responsibility Principle dictates that a class or module (or in the context of microservices, a service) should have only one reason to change, meaning it should only have one job or responsibility. In microservices, this ensures that each service does one thing and does it well, and interacts with others through clear interfaces.

Option A is incorrect. The Principle of Least Privilege is about ensuring that users or services have only the permissions they need to perform their tasks and nothing more. It's not specifically about the design of the service itself.

Option C is incorrect. The Open-Closed Principle is a design principle stating that software entities should be open for extension but closed for modification. While relevant for software design, it's not the primary principle guiding the design of individual microservices.

Option D is incorrect. The Zero Trust Model is a security concept where no one, whether inside or outside the organization, is trusted by default. It's not a principle specific to microservice design.

Question 579. A company's online retail website faces DDoS attacks that cause significant downtime. Their current setup relies on manual verification of traffic spikes before mitigation efforts are deployed. What change could BEST enhance the company's reaction time to such attacks in the future?

- (A) Educate users to report slow website loading times
- (B) Manually back up the website data every hour
- (C) **Deploy a web application firewall with automated DDoS mitigation features**
- (D) Increase the website's bandwidth to handle traffic spikes

Explanation 579. Correct Answer: C. Deploy a web application firewall with automated DDoS mitigation features. Deploying a web application firewall (WAF) with automated DDoS mitigation can instantly detect and mitigate

attack traffic, significantly improving reaction time to attacks compared to waiting for manual verification.

Option A is incorrect. Relying on users to report slow loading times is reactive and does not guarantee a swift response to DDoS attacks.

Option B is incorrect. Backing up website data is important for recovery, but it doesn't prevent or mitigate active DDoS attacks or improve reaction time.

Option D is incorrect. Merely increasing bandwidth might not be sufficient against DDoS attacks. An attacker can still overwhelm the increased capacity, and it doesn't address the need for swift detection and mitigation.

Question 580. A large enterprise is deploying a new automation system that will allow various teams, including development, operations, and QA, to provision and configure their own environments. The security team is concerned about potential misconfigurations or excessive permissions being granted. Which solution can be used within the automation to ensure security standards are met without limiting the agility of the teams?

- (A) Implementing a zero-trust model for all teams
- (B) Manually reviewing all requests before provisioning
- (C) **Setting up guard rails within the automation scripts to define boundaries and prevent misconfigurations**
- (D) Disabling the automation system for all teams except the security team

Explanation 580. Correct Answer: C. Setting up guard rails within the automation scripts to define boundaries and prevent misconfigurations. Guard rails in automation scripts act as safeguards, ensuring that certain actions, configurations, or provisions stay within defined security and operational boundaries without impeding the benefits of automation.

Option A is incorrect. While a zero-trust model is beneficial for security, it does not directly address the challenge of misconfigurations in automation processes.

Option B is incorrect. Manually reviewing all requests negates the efficiency benefits of automation and slows down the provisioning process.

Option D is incorrect. Disabling the automation system for all teams except the security team defeats the purpose of having an automation system for diverse teams and reduces agility.

Question 581. SecureNet, a cybersecurity firm, is implementing an Intrusion Detection System (IDS) for its enterprise client. Where should the IDS be placed for optimal detection of malicious activities?

(A) Before the perimeter firewall to capture all inbound traffic

(B) Between the perimeter firewall and the internal network to monitor the filtered traffic

(C) Inside the DMZ to monitor only external service requests

(D) Adjacent to each workstation for personalized security

Explanation 581. Correct Answer: B. Between the perimeter firewall and the internal network to monitor the filtered traffic. By placing the IDS between the firewall and the internal network, it can monitor traffic that has passed through the firewall's filters. This position provides a balance between capturing potential threats and reducing false positives from benign external traffic.

Option A is incorrect. While placing the IDS before the firewall will capture all inbound traffic, it may result in a high number of false positives since a lot of benign traffic might trigger alarms.

Option C is incorrect. Placing the IDS only in the DMZ would limit its visibility to only external service requests and not the overall internal traffic which might have potential threats.

Option D is incorrect. While personal IDS on each workstation provides granular monitoring, it does not provide a holistic view of network activities and can be resource-intensive.

Question 582. AlphaTech wants to ensure that its remote employees follow best security practices when working from home. The security team has been tasked with drafting a set of guidelines for remote work. What should be the primary focus of these guidelines?

- (A) Outlining punitive measures for non-compliance
- (B) Stating the company's legal position on remote work
- (C) **Recommending security measures for home networks and devices**

(D) Dictating the exact software and hardware specifications for remote workers

Explanation 582. Correct Answer: C. Recommending security measures for home networks and devices.

Guidelines aim to provide advice and recommendations. In the context of remote work, they would suggest best security practices for securing home networks and devices without being overly prescriptive.

Option A is incorrect. Punitive measures and compliance repercussions are typically outlined in policies or procedures, not guidelines.

Option B is incorrect. The company's legal position on remote work would be part of a policy or a legal document rather than a set of guidelines.

Option D is incorrect. Dictating exact software and hardware specifications would be more in line with standards rather than guidelines. Guidelines would provide broader recommendations.

Question 583. The incident response team at XYZ Corp received a report that an attacker successfully exploited a vulnerable web application in their environment. To identify which server might have been compromised, the team decided to cross-reference recent vulnerability scan results. Which of the following information from the vulnerability scan would be MOST helpful in pinpointing the potentially compromised server?

- (A) The timestamp of when the scan was conducted
- (B) The software version of the scanning tool
- (C) **List of hosts with the specific vulnerability related to the exploit**
- (D) The total number of vulnerabilities identified during the scan

Explanation 583. Correct Answer: C. List of hosts with the specific vulnerability related to the exploit. In the given scenario, to determine which server may have been compromised, the team should focus on those hosts identified in the vulnerability scan as having the specific vulnerability that matches the exploit used by the attacker.

Option A is incorrect. While the timestamp might indicate when the scan was done, it wouldn't provide specifics about which servers had the vulnerability related to the reported exploit.

Option B is incorrect. Knowing the software version of the scanning tool wouldn't assist in identifying the potentially compromised server.

Option D is incorrect. The total number of vulnerabilities identified doesn't help pinpoint a specific server; it only provides a high-level overview of the security posture.

Question 584. While conducting a routine security review, Jake, a security specialist, discovers an unexpected piece of data placed in the organization's financial system. Upon asking, he learns that this piece of data is intentionally placed and

monitored to see if any unauthorized user or system interacts with it. What is this deceptive piece of data known as?

- (A) Honeystring
- (B) **Honeytoken**
- (C) Canary token
- (D) Security marker

Explanation 584. Correct Answer: B. Honeytoken.

Honeytokens are strategically placed deceptive pieces of data that have no actual value or real-world use but are closely monitored. Their sole purpose is to detect unauthorized interactions, as any access or use of a honeytoken is likely malicious or unauthorized.

Option A is incorrect. There isn't a commonly recognized security term known as "Honeystring" in the context described.

Option C is incorrect. Canary tokens are a specific type of honeytoken and can serve the same purpose. However, given the choices provided and the context of the question, "Honeytoken" is the most accurate answer.

Option D is incorrect. A security marker, in a general sense, can be any mark or indicator used for security purposes, but it isn't specifically a deceptive piece of data placed to detect unauthorized access.

Question 585. DeltaCorp has a password policy in place which mandates users to change their passwords every 30 days. However, some users complain that this results in them choosing simpler passwords or writing them down to remember

them. How can DeltaCorp maintain security while addressing these concerns?

- (A) **Reduce the password change frequency but introduce more complexity requirements**
- (B) Eliminate password changes and rely solely on two-factor authentication
- (C) Ask users to change passwords every week to improve security
- (D) Allow users to reuse any of their last three passwords to ease the transition

Explanation 585. Correct Answer: A. Reduce the password change frequency but introduce more complexity requirements. By reducing the frequency of password changes, users are less burdened with the task of remembering new passwords frequently. Adding complexity requirements can compensate for the longer duration by ensuring that passwords are strong.

Option B is incorrect. Relying solely on two-factor authentication (2FA) without any password requirements can introduce risks if the 2FA method is compromised. Additionally, 2FA can be inconvenient for users if not implemented correctly.

Option C is incorrect. Asking users to change passwords even more frequently would exacerbate the issue and likely lead to even weaker password practices.

Option D is incorrect. Allowing users to reuse recent passwords undermines the purpose of having them change passwords in the first place and reduces overall security.

Question 586. A software company recently discovered a vulnerability in its popular application, which allowed unauthorized access to users' data. Before the company could release a patch, a group of hackers exploited the vulnerability but only to notify the users about it. They did not misuse any data. What is the most probable motivation behind this group's action?

- (A) Financial gain by selling the data
- (B) Political beliefs against the software company's operations
- (C) **Ethical concerns about user privacy and security**
- (D) Desire to disrupt the software company's services

Explanation 586. Correct Answer: C. Ethical concerns about user privacy and security. The hackers did not misuse the data but instead chose to inform the users about the vulnerability, suggesting their motivation was based on ethical considerations to ensure users are aware of potential threats to their privacy.

Option A is incorrect. The hackers did not sell or misuse the data, which means financial gain wasn't their primary objective.

Option B is incorrect. There's no indication that the hackers' actions were driven by political beliefs against the software company.

Option D is incorrect. While the hackers did exploit a vulnerability, they did not aim to disrupt the company's services but to inform users about the vulnerability.

Question 587. In a routine security assessment, Claire found that a newly deployed database server within her organization is still using its default login credentials. Which of the following is the PRIMARY security risk associated with this finding?

- (A) The database will not function optimally
- (B) The server will need frequent patches
- (C) **Unauthorized individuals may easily gain access**
- (D) The server will consume more bandwidth

Explanation 587. Correct Answer: C. Unauthorized individuals may easily gain access. Default credentials are often publicly known, and if they are not changed, malicious actors can easily use them to gain unauthorized access to systems.

Default credentials, which may include usernames and passwords set by manufacturers for initial setup, are widely known and can be easily searched online. If not changed after deployment, they pose a significant security risk as they allow anyone with this knowledge to gain access to the system.

Option A is incorrect. The use of default credentials doesn't directly impact the optimal functioning of the database.

Option B is incorrect. The use of default credentials doesn't mean that the server will need frequent patches. However, patch management is a separate aspect of maintaining server security.

Option D is incorrect. The use of default credentials doesn't directly cause the server to consume more bandwidth.

Question 588. DeltaTech, a progressive tech firm, is aiming to improve its security posture by eliminating the vulnerabilities associated with password use. They are considering deploying a passwordless authentication system. Which of the following represents the PRIMARY advantage of such a system?

- (A) It allows users to choose any password complexity
- (B) **It eliminates the need for remembering passwords**
- (C) It guarantees protection against all cyber threats
- (D) It ensures compatibility with all legacy systems

Explanation 588. Correct Answer: B. It eliminates the need for remembering passwords. Passwordless authentication methods, such as biometrics, hardware tokens, or mobile app confirmations, remove the need for users to remember and input passwords. This can reduce risks associated with weak or reused passwords and enhance user convenience.

Option A is incorrect. Passwordless systems remove the concept of a traditional password altogether, so there's no "password complexity" to choose.

Option C is incorrect. While passwordless authentication can significantly enhance security, especially against threats like password spraying or credential stuffing, it doesn't guarantee protection against all cyber threats.

Option D is incorrect. Passwordless authentication methods might not be compatible with all legacy systems without modifications or updates.

Question 589. A financial institution recently discovered that a large number of confidential customer records were being accessed and copied during off-business hours. Upon investigation, it was found that the access came from an authenticated user within the company, who had recently been passed over for a promotion. Which type of threat actor is MOST likely responsible for this security incident?

- (A) Hacktivist
- (B) **Insider threat**
- (C) Nation-state
- (D) Organized crime syndicate

Explanation 589. Correct Answer: B. Insider threat. The evidence suggests the activities were conducted by an authenticated user within the organization, who might have a motive (having been passed over for a promotion). Insider threats are risks from individuals within the organization such as employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems.

Option A is incorrect. Hacktivists are typically motivated by political or social causes and will target organizations to promote or protest a specific issue. They are not usually motivated by personal grievances like being passed over for promotions.

Option C is incorrect. Nation-states are driven by political, espionage, or military objectives. Accessing customer records of a financial institution for personal reasons doesn't align with their typical motivations.

Option D is incorrect. While organized crime syndicates might have an interest in customer records for financial gains, the inside access and the motive related to a missed promotion strongly suggest an insider threat.

Question 590. A financial institution wants to ensure that customers are aware of the bank's policies on information sharing and how their personal data is used. Which of the following security controls would BEST communicate this to customers?

- (A) Implementing end-to-end encryption for online transactions
- (B) **Publishing a privacy policy on the bank's website**
- (C) Conducting annual cybersecurity awareness training for employees
- (D) Using multi-factor authentication for online banking

Explanation 590. Correct Answer: B. Publishing a privacy policy on the bank's website. A privacy policy serves as a directive control as it informs customers about the bank's practices regarding the collection, use, and sharing of their personal data. By reading the policy, customers understand their rights and the bank's responsibilities.

Option A is incorrect. While end-to-end encryption ensures the confidentiality of online transactions, it doesn't inform customers about the bank's policies on information sharing or how their data is used.

Option C is incorrect. Annual cybersecurity awareness training is aimed at employees, not customers. It wouldn't directly

communicate the bank's information-sharing policies to its customers.

Option D is incorrect. Using multi-factor authentication improves the security of online banking by requiring multiple forms of verification. However, it doesn't communicate to customers how their personal data is used or the bank's information-sharing policies.

Question 591. OmegaHealth, a large healthcare provider, is integrating automation into its operations. When a new healthcare worker is hired, they require access to multiple systems. Why would OmegaHealth automate the user provisioning process across these systems?

- (A) To enforce a uniform password for all healthcare workers.
- (B) **To save time by ensuring consistent and simultaneous account creation across all necessary platforms**
- (C) To prevent the new hires from accessing any system until their probation period ends
- (D) To reduce the software licenses needed by delaying account activation

Explanation 591. Correct Answer: B. To save time by ensuring consistent and simultaneous account creation across all necessary platforms. Automating user provisioning, especially in an environment where access to multiple systems is needed, can dramatically save time and reduce human errors. With automation, accounts can be created consistently and simultaneously across all required platforms.

Option A is incorrect. Enforcing a uniform password for all users is a poor security practice. Automation should focus on efficiency and security, not creating potential vulnerabilities.

Option C is incorrect. Automating user provisioning doesn't inherently prevent new hires from accessing systems. The automation should be designed to provision based on specific rules and roles.

Option D is incorrect. Automation in user provisioning is about streamlining the creation and management of accounts, not about reducing software licenses or delaying activations.

Question 592. After detecting an unauthorized intrusion into their network, a financial institution wants to implement a control that will restore compromised systems to a known good state. Which of the following would be the MOST appropriate corrective control?

- (A) Implementing Intrusion Detection Systems (IDS) across the network
- (B) Frequently updating firewall rules
- (C) **Restoring systems from verified backups**
- (D) Enabling multi-factor authentication for users

Explanation 592. Correct Answer: C. Deploying infrared (IR) sensors. Infrared (IR) sensors detect infrared radiation, such as the heat emitted by the human body. This makes them particularly effective in detecting human intruders, even in complete darkness, based on the body heat they emit.

Option A is incorrect. While CCTV cameras with LED lights can provide visual surveillance, they rely on light to produce images and may not detect intruders in complete darkness as efficiently as infrared sensors.

Option B is incorrect. Ultrasonic motion sensors detect movement through sound waves, not body heat, making them less efficient in differentiating between a human intruder and other moving objects.

Option D is incorrect. RFID badge readers control access at entry points but do not detect human intruders based on their body heat inside a facility.

Question 593. Maria receives a text message on her phone from an unknown number, stating that she has won a gift card worth \$500 from a popular online store. The message includes a link asking her to click on it to claim her prize. Maria is unsure about the authenticity of the message. Which of the following is the BEST course of action for Maria?

- (A) Click the link to check if the website looks genuine
- (B) Forward the message to her friends to verify if they received a similar message
- (C) **Delete the message without clicking on any links**
- (D) Respond to the sender asking for more details about the offer

Explanation 593. Correct Answer: C. Delete the message without clicking on any links. Messages from unknown sources, especially those that sound too good to be true, often

signal a potential security threat. It's safest to delete such messages without interacting with any links.

Smishing is a type of phishing attack wherein attackers use SMS to deceive users into divulging personal information, visiting a malicious website, or downloading malware onto their smartphones. Users should always be cautious of unsolicited messages from unknown numbers.

Option A is incorrect. Clicking the link, even out of curiosity, can lead to a malicious website or download malware onto Maria's device.

Option B is incorrect. While forwarding the message to friends might give her insight into its authenticity, it could also expose her friends to potential threats if the message is malicious.

Option D is incorrect. Responding to the sender could give them more information about Maria or confirm that her number is active, leading to further targeted attacks.

Question 594. In preparation for a potential lawsuit, Meg, a cybersecurity analyst, has been asked to ensure that specific digital evidence remains intact and is not altered or deleted. What measure should Meg implement to ensure this requirement?

- (A) Encrypt the evidence
- (B) **Initiate a legal hold**
- (C) Perform a full disk wipe
- (D) Conduct a vulnerability assessment

Explanation 594. Correct Answer: B. Initiate a legal hold. A legal hold ensures that specific data that could be relevant to a legal case is preserved and not altered or deleted until the hold is lifted. In this situation, Meg would initiate a legal hold to keep the digital evidence intact for the potential lawsuit.

Option A is incorrect. Encrypting the evidence can ensure its confidentiality, but it does not prevent deletion or guarantee its preservation for legal reasons.

Option C is incorrect. Performing a full disk wipe would eliminate all data on a disk, which is contrary to the requirement of preserving specific digital evidence.

Option D is incorrect. Conducting a vulnerability assessment is about identifying weaknesses in a system, not about preserving digital evidence for legal purposes.

Question 595. In an IaaS (Infrastructure as a Service) model, which of the following tasks is typically the responsibility of the cloud customer in a standard Cloud Responsibility Matrix?

- (A) Physical security of data centers
- (B) Patching of host operating systems
- (C) Network infrastructure maintenance
- (D) **Patching of guest operating systems**

Explanation 595. Correct Answer: D. Patching of guest operating systems. In an IaaS model, the customer is typically responsible for managing their own virtual machines, which includes patching the guest operating systems. The cloud

provider is generally responsible for the physical infrastructure, network, and the host operating system.

Option A is incorrect. Physical security of data centers is the responsibility of the cloud provider. The customer does not have control over the physical infrastructure in a cloud environment.

Option B is incorrect. Patching of host operating systems is the cloud provider's responsibility. They manage the underlying infrastructure, including the host systems.

Option C is incorrect. Maintenance of network infrastructure is typically handled by the cloud provider, ensuring connectivity and uptime for the resources they offer.

Question 596. A company detected a DDoS attack that lasted for several weeks. The attackers used a botnet of millions of infected devices and frequently rotated attack vectors to bypass mitigation efforts. This prolonged and resource-intensive attack suggests which kind of threat actor's resources and funding?

- (A) Amateur hacker with minimal resources
- (B) Cybersecurity researcher testing vulnerabilities
- (C) Nation-state actor with strategic interests
- (D) **Organized crime syndicate with substantial funding**

Explanation 596. Correct Answer: D. Organized crime syndicate with substantial funding. The scale and duration of the DDoS attack, combined with the use of a massive botnet and frequent rotation of attack vectors, point to a threat actor with significant resources. While nation-states could conduct such attacks, DDoS campaigns are also a hallmark of well-

funded organized crime syndicates, especially when financial or strategic extortion could be a motive.

Option A is incorrect. An amateur hacker with minimal resources would not have the capability to sustain a large-scale DDoS attack using a botnet of millions of devices over several weeks.

Option B is incorrect. Cybersecurity researchers typically do not engage in malicious activities, and launching a prolonged DDoS attack would be unethical and illegal.

Option C is incorrect. While a nation-state actor might have the resources to launch such an attack, DDoS attacks, especially those of extortion nature, are more commonly associated with organized crime syndicates.

Question 597. An art gallery wants to deploy a security solution to detect movement in an open courtyard that features several sculptures. This space has varying temperature conditions, which might cause false alarms in some motion detection technologies. Which type of sensor would be MOST appropriate to ensure consistent motion detection in such conditions?

- (A) Thermal imaging sensors
- (B) Pressure-sensitive mats
- (C) Ultrasonic detectors
- (D) **Microwave motion detectors**

Explanation 597. Correct Answer: D. Microwave motion detectors. Microwave motion detectors are suitable for open

areas and are less affected by temperature changes. They emit microwave beams to create an invisible detection zone and can consistently detect motion when an object interrupts this zone, irrespective of the ambient temperature.

Option A is incorrect. Thermal imaging sensors detect variations in heat. While they can be effective, the varying temperature conditions in the courtyard may cause inconsistencies in detection.

Option B is incorrect. Pressure-sensitive mats are designed to detect weight or pressure changes when stepped on. They would not be suitable for an open courtyard where movement needs to be detected across a larger area.

Option C is incorrect. Ultrasonic detectors emit sound waves to detect motion. However, they might also be affected by external environmental factors and are not as suitable for open courtyards as microwave motion detectors.

Question 598. TechBlitz Inc. recently underwent an IT audit, and one of the suggestions was to reduce the attack surface. Which of the following measures would be MOST effective in accomplishing this?

- (A) Increasing the password length requirement for all users
- (B) Implementing regular vulnerability assessments
- (C) **Deactivating unused services and ports on servers**
- (D) Implementing a strict BYOD (Bring Your Own Device) policy

Explanation 598. Correct Answer: C. Deactivating unused services and ports on servers. Reducing the number of active services and ports directly diminishes the number of potential entry points for attackers, thus reducing the attack surface.

Option A is incorrect. While increasing password length improves security against brute-force attacks, it doesn't directly affect the attack surface.

Option B is incorrect. Regular vulnerability assessments identify potential security gaps, but simply identifying doesn't reduce the attack surface unless actions are taken based on findings.

Option D is incorrect. A strict BYOD policy can enhance security, but it's focused more on the types of devices and how they connect rather than reducing the number of potential attack points.

Question 599. A user receives an SMS claiming to be from her bank, alerting her of unauthorized activity on her account. The message instructs the user to immediately click on a provided link and verify her account details. The user hasn't noticed any irregularities with her bank account. Which type of attack is this SMS most likely part of?

- (A) **Smishing**
- (B) Vishing
- (C) Bluejacking
- (D) Bluesnarfing

Explanation 599. Correct Answer: A. Smishing. Smishing is a type of phishing attack where malicious actors use SMS to deceive individuals into providing sensitive information, typically by impersonating trusted organizations or contacts.

Option B is incorrect. Vishing refers to voice phishing, where attackers use voice calls instead of text or email to impersonate legitimate entities and scam victims.

Option C is incorrect. Bluejacking involves sending unsolicited messages to Bluetooth-enabled devices. It doesn't typically involve impersonating a legitimate entity for deceptive purposes.

Option D is incorrect. Bluesnarfing is a type of unauthorized access to or theft of information from a Bluetooth device. It doesn't involve deceptive SMS messages.

Question 600. After a recent security breach, CyberCorp is reviewing its software vendors for their responsiveness to vulnerabilities. Which of the following metrics would BEST assist CyberCorp in determining the timeliness and efficiency of security patches from a vendor?

- (A) The frequency of software updates released by the vendor
- (B) The vendor's quarterly financial reports
- (C) **Time between vulnerability disclosure and patch release by the vendor**
- (D) The number of features added by the vendor in the last software update

Explanation 600. Correct Answer: C. Time between vulnerability disclosure and patch release by the vendor. The time taken by a vendor to release a security patch after a vulnerability is disclosed is a direct measure of their responsiveness to security threats. A shorter duration indicates a higher prioritization of security concerns.

Option A is incorrect. Frequency of software updates does not necessarily correlate with timely security patches. A vendor might release frequent updates but still be slow in addressing security issues.

Option B is incorrect. A vendor's quarterly financial reports might indicate the financial health of the company but does not directly reflect their responsiveness to security vulnerabilities.

Option D is incorrect. The number of features added in a software update does not indicate the timeliness or effectiveness of security patches.

BONUSES & DISCOUNTS

Enrich your online experience with ExamsDigest.

Your purchase of this product includes free access to online practice exam simulators on examsdigest.com. You will have access for one (1) month. You may also access our full library of Practice exams and share with other learners. Send us an email to info@examsdigest.com now and start your online practice experience!

Your purchase includes:

- ✓ Access to online simulators for 1 month
- ✓ Up to 20% discount on Exam Voucher
- ✓ \$10 OFF on [ExamsDigest Marketplace](#)

About ExamsDigest.

xDigest is a consortium of brands committed to offering top-tier online training for the most sought-after IT certifications including, but not limited to, CompTIA, Amazon, Cisco, and Google. We furnish a range of educational resources such as exam simulators, coding exercises, Linux training, Performance-Based Questions (PBQs), practical labs, and concise study guides.