CompTIA

SECURITY+

EXAM SY0-701

PRACTICE TESTS

www.bootcampinsight.com

CompTIA Security+ sy0-701 exam questions for Practice

01. Question: What type of access control model uses policies that evaluate attributes (user, resource, and environment) to make access decisions?

(A) Mandatory Access Control (MAC)

(B) Discretionary Access Control (DAC)

(C) Role-Based Access Control (RBAC)

(D) Attribute-Based Access Control (ABAC)

Correct Answer: (D) Attribute-Based Access Control (ABAC)

Explanation: Attribute-Based Access Control (ABAC) is an access control model that evaluates attributes or characteristics of user, resource, and environment, against policies, to make access decisions. This model provides a high level of flexibility and granularity, making it suitable for complex and dynamic environments.

02. Question: Which principle ensures that critical decisions are not dependent on a single individual?

(A) Dual Control

(B) Need to Know

(C) Separation of Duties

(D) Least Privilege

Correct Answer: (C) Separation of Duties

Explanation: Separation of duties is a security principle designed to reduce the risk of fraud and error by dividing critical processes and tasks among multiple individuals. This ensures that no single individual has the authority or ability to complete all components of a critical task on their own, thus preventing misuse of power and enhancing security.

03. Question: What security concept involves disguising data to hide its true content?

(A) Encryption

(B) Obfuscation

(C) Tokenization

(D) Anonymization

Correct Answer: (B) Obfuscation

Explanation: Obfuscation is the practice of making something difficult to understand or interpret, often used in the context of making code or data harder to decipher. This can deter attackers by concealing the actual code or data structure, although it is not a substitute for strong encryption techniques.

04. Question: Which of the following best defines the concept of 'availability' in the context of information security?

(A) Ensuring timely and reliable access to and use of information
(B) Preventing unauthorized access to information
(C) Ensuring the accuracy and completeness of information
(D) Guaranteeing the confidentiality of information
Correct Answer: (A) Ensuring timely and reliable access to and use of information

Explanation: Availability, as part of the CIA triad (Confidentiality, Integrity, Availability), focuses on ensuring that authorized users have timely and reliable access to information and computing resources as required for their tasks. This is crucial for maintaining operational effectiveness and preventing disruptions to business processes.

05. Question: Which type of security control attempts to discourage security violations before they occur?

(A) Preventive

(B) Detective

(C) Corrective

(D) Deterrent

Correct Answer: (D) Deterrent

Explanation: Deterrent controls are designed to discourage individuals from violating security policies or procedures by warning of the negative consequences of doing so. These controls serve as a psychological barrier rather than physically preventing or detecting security breaches.

06. Question: What term is used to describe the unauthorized tracking of RFID tags?

(A) Eavesdropping

(B) Phishing

(C) Skimming

(D) Spoofing

Correct Answer: (C) Skimming

Explanation: Skimming refers to the unauthorized capture or tracking of RFID and magnetic stripe data from payment cards, identification cards, and passports. It's a form of electronic pickpocketing where attackers can steal information without physically touching the card or tag.

07. Question: Which security model is specifically designed to prevent conflict of interest when accessing data?

(A) Bell-LaPadula Model

(B) Biba Model

(C) Clark-Wilson Model

(D) Brewer and Nash Model

Correct Answer: (D) Brewer and Nash Model

Explanation: The Brewer and Nash Model, also known as the Chinese Wall Model, is designed to prevent conflicts of interest by restricting users' access to information based on their prior access to potentially competitive or conflicting data. This model helps maintain data confidentiality in environments where information barriers are necessary.

08. Question: Which of the following best describes a 'man-in-the-middle' (MITM) attack?

(A) An attack where the perpetrator secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

(B) An attack that involves flooding a targeted machine or resource with excessive requests to overload systems and prevent some or all legitimate requests from being fulfilled.

(C) A form of cyber attack that uses disguised email as a weapon. The goal is to tEthan the email recipient into believing that the message is something they want or need.

(D) An attack where the attacker secretly intercepts and logs all the victim's outgoing messages.

Correct Answer: (A) An attack where the perpetrator secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Explanation: A man-in-the-middle (MITM) attack involves an attacker inserting themselves into a conversation between two parties, impersonating both to intercept, send, and receive data intended for someone else, without either party knowing that there is an intruder.

09. Question: What is the primary security concern with 'shadow IT'?

(A) Increased costs due to unapproved software purchases

(B) Legal issues arising from unlicensed software use

(C) Security risks due to lack of oversight and management

(D) Decreased productivity due to non-standard software solutions

Correct Answer: (C) Security risks due to lack of oversight and management

Explanation: 'Shadow IT' refers to IT devices, software, and services outside the ownership or control of IT departments. The main concern is

the security risk it poses, as these can include unsecured applications, devices, and services that have not been vetted by the organization's security protocols, potentially leading to data breaches.

10. Question: What does a 'blacklist' access control strategy involve?

(A) Allowing access to all resources, except those specifically denied.

(B) Denying access to all resources, except those specifically allowed.

(C) Granting access based on the user's role within the organization.

(D) Allowing access based on the sensitivity of the information.

Correct Answer: (A) Allowing access to all resources, except those specifically denied.

11. Question: A security team is concerned about the potential for data leaks through cloud storage services used by employees. Which of the following strategies would MOST effectively mitigate this risk?

(A) Blocking access to all cloud storage services

(B) Encrypting all data stored in the cloud

(C) Implementing a Cloud Access Security Broker (CASB)

(D) Training employees on the proper use of cloud storage

Correct Answer: (C) Implementing a Cloud Access Security Broker (CASB)

Explanation: Implementing a CASB allows an organization to monitor and control the use of cloud services, including cloud storage, by providing visibility, compliance, data security, and threat protection. While blocking access, encrypting data, and training employees are useful measures.

12. Question: Sara, while investigating a security incident, checks the **/var/log** directory on a Linux system and discovers the **audit.log** file to be empty, despite the system having been up for over a month. What scenario has she most likely stumbled upon?

(A) Log files have been wiped

(B) The system was recently rebooted

(C) There was a system error

(D) She lacks the correct permissions to view the log

Correct Answer: (A) Log files have been wiped

Explanation: Sara's finding suggests that the audit logs have been intentionally cleared, a common tactic by intruders to cover their tracks after gaining privileged access. This action warrants concern as it implies a deliberate attempt to remove evidence of unauthorized activities. System reboots don't erase **audit.log**, and while system errors might cause logging issues, they don't result in empty logs without a trace. Permission issues could prevent log viewing but wouldn't explain an empty **audit.log**, reinforcing the suspicion of a wipe.

13. Question: When evaluating concerns related to the hardware supply chain, which of the following is LEAST likely to be a prevalent issue?

(A) Pre-installed malware on hardware

(B) Shortages in hardware availability

(C) Unauthorized modifications by third parties

(D) Malicious alterations to firmware

Correct Answer: (C) Unauthorized modifications by third parties

Explanation: While pre-installed malware, firmware tampering, and hardware availability are significant concerns within the hardware supply chain, unauthorized third-party modifications are relatively rare compared to the other listed threats. The main risks usually stem from the initial supply chain stages, including manufacturing and distribution, rather than later third-party alterations.

14. Question: Evan is evaluating the motivations behind potential internal threat actors within his organization. Which motivation is MOST likely to drive such an individual?

(A) Engaging in espionage

(B) Acting out of blackmail

(C) Participating in warfare

(D) Holding strong political convictions

Correct Answer: (B) Acting out of blackmail

Explanation: Internal threats often arise from motivations like financial gain, revenge, or as a response to blackmail, rather than the more ideologically driven motives of espionage, warfare, or political activism, which are typically associated with external threat actors such as nation-states or hacktivists. Blackmail can coerce employees into acting against their organization, making it a crucial concern for internal security assessments.

15. Question: Sophia notices an anomaly in login activities: an employee appears to have logged in from China and then from the United Kingdom within a single hour. How should this be categorized in terms of security concerns?

(A) Misuse of concurrent sessions

(B) Resource access issues

(C) Impossible travel activity

(D) Network segmentation breach

Correct Answer: (C) Impossible travel activity

Explanation: The described scenario is a classic example of "impossible travel," a security red flag indicating that logins are happening from geographically implausible locations in a short timeframe. This could suggest compromised credentials or other security issues, as physically traveling between such distant locations in the time frame described is not feasible. VPN use might explain such activity, but the lack thereof here hints at a security compromise.

16. Question : James is required to enter a 6-digit PIN in addition to using his RFID badge at his workplace. What security threat is this additional measure aiming to mitigate?

(A) Tailgating

(B) Man-in-the-path attacks

(C) Simultaneous access breaches

(D) Cloning of RFID badges

Correct Answer: (D) Cloning of RFID badges

Explanation: The requirement for a PIN in addition to an RFID badge is a strategy to combat badge cloning, ensuring that physical access control systems aren't compromised solely through duplicated RFID badges. While tailgating and concurrent access present security challenges, they involve different vulnerabilities and countermeasures. Man-in-the-path (or on-path) attacks relate to data interception, not physical access control, making badge cloning the primary concern addressed by the PIN requirement.

Explanation: The requirement for a PIN in addition to an RFID badge is a strategy to combat badge cloning, ensuring that physical access control systems aren't compromised solely through duplicated RFID badges. While tailgating and concurrent access present security challenges, they involve different vulnerabilities and countermeasures. Man-in-the-path (or on-path) attacks relate to data interception, not physical access control, making badge cloning the primary concern addressed by the PIN requirement.

17. Question: Ethan discovers that traffic from one of their domains is being redirected to a competitor's site, with administrative details altered. Assuming the domain hasn't expired, what likely happened?

(A) DNS hijacking

(B) Man-in-the-path attack

(C) Domain hijacking

(D) Exploitation of an unknown vulnerability (zero-day attack)

Correct Answer: (C) Domain hijacking

Explanation: The alteration of domain registration and administrative details without the owner's consent is indicative of domain hijacking. This act, distinct from DNS hijacking, involves unauthorized changes at the registrar level, allowing attackers to redirect or misuse the domain. While DNS hijacking affects domain name resolution, and on-path attacks intercept or modify data in transit, domain hijacking directly compromises domain ownership. Zero-day attacks refer to previously unknown software vulnerabilities, not directly related to the manipulation of domain registration information.

18. Question: An organization finds that certain outbound traffic is being redirected through an unauthorized IP address. What type of security breach is this indicative of?

- (A) DNS Spoofing
- (B) Service Denial
- (C) Insider Threat
- (D) Physical Security Breach

Correct Answer: (A) DNS Spoofing

Explanation: DNS Spoofing, or DNS cache poisoning, involves altering DNS entries to redirect traffic to malicious sites or intercept data. This type of attack manipulates the way domain names are resolved to reroute traffic, unlike service denial attacks that disrupt service availability, insider threats involving malicious actions by organization members, or physical breaches impacting tangible assets.

19. Question: During a routine audit, an admin discovers several user accounts with unusually high privileges not required for their job roles. What principle is being violated?

(A) Principle of Least Privilege

(B) Segregation of Duties

(C) Need to Know

(D) Continuous Monitoring

Correct Answer: (A) Principle of Least Privilege

Explanation: The Principle of Least Privilege dictates that users should have only the minimum level of access or permissions necessary to perform their job functions. Excessively high privileges can increase the risk of internal misuse or exploitation by attackers, whereas Segregation of Duties involves dividing tasks to prevent fraud and errors, Need to Know restricts access to information, and Continuous Monitoring relates to ongoing surveillance of system activities.

20. Question: An organization's IT department notices slow network performance and traces the issue to a large volume of outbound SMTP traffic. What kind of compromise does this suggest?

(A) Man-in-the-Middle Attack

(B) Distributed Denial of Service (DDoS) Attack

(C) Email Server Compromise

(D) Phishing Attack

Correct Answer: (C) Email Server Compromise

Explanation: A surge in outbound SMTP traffic can indicate an email server compromise, where attackers may use the server to distribute spam or malicious emails. Unlike Man-in-the-Middle attacks that intercept communications, DDoS attacks that flood services with excessive requests, or phishing attacks aimed at deceiving recipients, an email server compromise directly affects the ability to control outbound email traffic.

21. Question: A security analyst notices an uptick in encrypted traffic bypassing the organization's secure web gateway. What might be occurring?

(A) SSL Stripping

(B) Encrypted Malware Transmission

(C) Certificate Authority Compromise

(D) Rogue VPN Usage

Correct Answer: (D) Rogue VPN Usage

Explanation: The increase in encrypted traffic bypassing security measures like a secure web gateway could indicate rogue VPN usage, where users or attackers are circumventing organizational security policies and controls. SSL Stripping downgrades secure connections, encrypted malware transmission involves malware hidden in encrypted traffic (but wouldn't necessarily bypass gateways), and Certificate Authority Compromise impacts the integrity of digital certificates, differing from the direct bypassing of security infrastructure indicated by rogue VPN usage.

Question 22: Evelyn wants to deploy an encryption solution that will protect files in motion as they are copied between file shares, as well as at rest, and also needs it to support granular per-user security. What type of solution should she select?

A. Partition encryption

B. File encryption

C. Full-disk encryption

D. Record-level encryption

Correct Answer: B. File encryption

Explanation: File encryption allows for the protection of individual files both in transit and at rest, offering granular control over who can access specific files, making it the best choice for Evelyn's requirements.

Question 23: Valerie wants to use a certificate to handle multiple subdomains for her website, including sales.example.com and support.example.com. What type of certificate should she use?

A. A self-signed certificate

B. A root of trust certificate

C. A CRL certificate

D. A wildcard certificate

Correct Answer: D. A wildcard certificate

Explanation: A wildcard certificate is used to secure a base domain and an unlimited number of subdomains, making it suitable for Valerie's need to cover sales.example.com and support.example.com under one certificate.

Question 24: What information is analyzed during a gap analysis?

A. Control objectives and controls intended to meet the objectives

B. Physically separate networks and their potential connection points

C. Compensating controls and the controls they are replacing

D. Security procedures and the policies they are designed to support

Correct Answer: A. Control objectives and controls intended to meet the objectives

Explanation: A gap analysis involves comparing actual performance with potential or desired performance; in the context of security, this means analyzing the current controls against the control objectives to identify gaps.

Question 25: Casey's team has recommended an application restart for a production customer-facing application as part of an urgent patch due to a security update. What technical implication is the most common concern when conducting an application restart?

A. Application configuration changes caused by the restart

B. Whether the patch will properly apply

C. Lack of security controls during the restart

D. The downtime during the restart

Correct Answer: D. The downtime during the restart

Explanation: The most common concern with restarting an application, especially a customer-facing one, is the downtime involved, which can impact user access and service availability.

Question 26: Using a tool like git is most frequently associated with what critical change management process?

A. Having a backout plan

B. Stakeholder analysis

C. Version control

D. Standard operating procedures (SOPs)

Correct Answer: C. Version control

Explanation: Git is a version control system used for tracking changes in source code during software development, making it an essential tool for managing versions of code and documents in a change management process.

Question 27: Evelyn is concerned that the password used for one of his organization's services is weak, and he wants to make it harder to crack by making it harder to test possible keys during a brute-force attack. What is this technique called?

A. Master keying

B. Key stretching

C. Key rotation

D. Passphrase armoring

Correct Answer: B. Key stretching

Explanation: Key stretching is a technique used to make brute-force attacks more difficult by applying an algorithm to a password which makes its hashing process computationally more demanding.

Question 28: Log monitoring is an example of what control category?

A. Technical
B. Managerial
C. Operational
D. Physical

Correct Answer: A. Technical

Explanation: Log monitoring is a technical control that involves the use of software tools to automatically monitor and analyze computer logs for security and operational issues.

Question 29: James wants to make offline brute-force attacks against his password file very difficult for attackers. Which of the following is NOT a common technique to make passwords harder to crack?

A. Use of a salt

B. Use of a pepper

C. Use of a purpose-built password hashing algorithm

D. Encrypting password plaintext using symmetric encryption

Correct Answer: D. Encrypting password plaintext using symmetric encryption

Explanation: Encrypting password plaintext is not a method to make passwords harder to crack in the context of storing password hashes. Salting, peppering, and using secure hashing algorithms are common techniques to secure passwords against offline brute-force attacks.

Question 30: Diffie-Hellman and RSA are both examples of what important encryption-related solution?

A. Rekeying

B. Certificate revocation protocols

C. Key exchange algorithms

D. Key generation algorithms

Correct Answer: C. Key exchange algorithms

Explanation: Diffie-Hellman and RSA (Rivest-Shamir-Adleman) are both used for secure key exchange over an insecure medium, allowing parties to establish a shared secret key for encryption.

Question 31: Emma wants to ensure that her change management process includes a procedure for what to do if the change fails. What should she create to handle this possibility?

A. An impact analysis

B. A backout plan

C. A regression test

D. A maintenance window

Correct Answer: B. A backout plan

Explanation: A backout plan is a critical component of change management, detailing the steps to revert changes if they result in unexpected issues or failures, ensuring system stability is maintained.

Question 32: A rapidly growing e-commerce company has recently experienced an increase in cross-site scripting (XSS) and SQL injection attacks. To specifically combat these types of threats at the application layer, which firewall solution is most suitable?

(A) Stateful Packet Inspection Firewall

(B) Proxy Firewall

(C) Network Layer Firewall

(D) Web Application Firewall (WAF)

Correct Answer: (D) Web Application Firewall (WAF)

Explanation: A Web Application Firewall (WAF) is designed to monitor, filter, and block harmful HTTP traffic to web applications. It provides defense against common web application threats such as XSS and SQL injection attacks by inspecting HTTP requests.

Question 33: SafeGaurdPlus, a cybersecurity firm, is tasked with deploying an Intrusion Detection System (IDS) for an enterprise client. Where should the IDS be positioned to optimally detect malicious activity?

(A) Before the perimeter firewall to capture all inbound traffic

(B) Between the perimeter firewall and the internal network to monitor filtered traffic

(C) Inside the DMZ to monitor only external service requests

(D) Adjacent to each workstation for personalized security

Correct Answer: (B) Between the perimeter firewall and the internal network to monitor filtered traffic

Explanation: Placing the IDS between the perimeter firewall and the internal network allows it to scrutinize traffic that has been filtered by the firewall. This strategic placement helps in identifying potential threats while minimizing false positives from harmless external traffic.

Question 34: ABC Corp's software development team has developed an application with unique and innovative algorithms. To prevent competitors from copying or replicating their application's functionality, what legal protection should the company seek?

(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)

Correct Answer: (B) Apply for a patent for the innovative algorithms

Explanation: Securing a patent for the innovative algorithms grants ABC Corp the exclusive rights to their invention, thereby legally protecting it from being copied or used by competitors, aligning with the goal of safeguarding the application's unique functionalities.

Question 35: When designing services in a microservices architecture, what principle ensures each service performs a specific task and interacts with others through well-defined interfaces?

(A) Principle of Least Privilege

(B) Single Responsibility Principle

(C) Open-Closed Principle

(D) Zero Trust Model

Correct Answer: (B) Single Responsibility Principle

Explanation: The Single Responsibility Principle mandates that a service should have only one responsibility or function. This principle ensures that each service in a microservices architecture is focused on a specific task and interacts with other services through clear and well-defined interfaces.

Question 36: A multinational organization with multiple branch offices seeks a technology to simplify their WAN connectivity, reduce costs, and ensure secure data transfers between offices. Which technology best fits their needs?

(A) VLAN

(B) MPLS

(C) SD-WAN

(D) DMZ

Correct Answer: (C) SD-WAN

Explanation: Software-defined WAN (SD-WAN) enables the use of multiple transport services, including MPLS, LTE, and broadband, for secure and efficient connectivity. It offers cost savings by utilizing lower-cost internet connections and simplifies WAN management, making it ideal for the organization's requirements.

Question 37: A financial company aims to improve web browsing security by intercepting web traffic to prevent access to malicious sites and malware downloads. What solution acts as an intermediary for client resource requests?

(A) Network IDS

(B) VPN Concentrator

(C) Proxy server

(D) Jump server

Correct Answer: (C) Proxy server

Explanation: A Proxy server acts as a mediator between users and the internet, intercepting requests to provide functions like content filtering, request caching, and security inspection, thereby enhancing web browsing security by preventing access to harmful sites.

Question 38: What is the primary purpose of conducting regular security audits within an organization?

(A) To monitor employee productivity levels

(B) To ensure compliance with security policies and regulations

(C) To evaluate the performance of IT infrastructure

(D) To manage employee access to social media

Correct Answer: (B) To ensure compliance with security policies and regulations

Explanation: Regular security audits are conducted to assess and ensure that the organization's security measures are in compliance with internal security policies as well as external regulations and standards. This helps identify vulnerabilities, ensures security controls are functioning as intended, and demonstrates due diligence in protecting sensitive information.

Question 39: In incident response, what is the FIRST step that should be taken after identifying a security breach?

(A) Eradication of the threat

(B) Containment of the breach

(C) Notification of stakeholders

(D) Recovery of affected systems

Correct Answer: (B) Containment of the breach

Explanation: The first step in responding to a security breach is to contain it, preventing further spread or damage. Containment strategies may vary depending on the nature of the breach but are critical to limiting the impact on the organization's operations and data integrity.

Question 40: Which tool is MOST effective for detecting unauthorized changes to software and system configurations?

(A) Antivirus software

(B) Intrusion Detection System (IDS)

(C) File Integrity Monitoring (FIM) tools

(D) Firewalls

Correct Answer: (C) File Integrity Monitoring (FIM) tools

Explanation: File Integrity Monitoring (FIM) tools are specifically designed to detect changes in files, configurations, and logs, alerting administrators to unauthorized modifications that could indicate a security breach or policy violation. These tools are crucial for maintaining the security and integrity of critical systems.

Question 41: Which of the following best describes the role of a Security Operations Center (SOC)?

(A) Developing and enforcing the organization's security policies

(B) Designing the organization's network architecture

(C) Monitoring, detecting, analyzing, and responding to cybersecurity incidents

(D) Managing the organization's IT infrastructure

Correct Answer: (C) Monitoring, detecting, analyzing, and responding to cybersecurity incidents

Explanation: A Security Operations Center (SOC) is a centralized unit within an organization that deals with security issues on an organizational and technical level. It is responsible for continuously monitoring and analyzing the organization's security posture while detecting, analyzing, and responding to cybersecurity incidents.

Question 42: What is the primary goal of implementing a Security Information and Event Management (SIEM) system?

(A) To encrypt sensitive data

(B) To provide real-time analysis of security alerts generated by applications and network hardware

(C) To manage network devices and configurations

(D) To conduct vulnerability scans on the network

Correct Answer: (B) To provide real-time analysis of security alerts generated by applications and network hardware

Explanation: A Security Information and Event Management (SIEM) system collects and aggregates log data generated across the organization's technology infrastructure, from network devices to applications, providing real-time analysis of security alerts to identify and respond to threats swiftly.

Question 43: In the context of digital forensics, what is the primary importance of maintaining a chain of custody for evidence?

(A) To ensure the evidence can be safely stored for long periods

(B) To document the evidence's control, transfer, analysis, and disposition

(C) To increase the efficiency of the forensic analysis

(D) To ensure the privacy of individuals involved in the investigation

Correct Answer: (B) To document the evidence's control, transfer, analysis, and disposition

Explanation: Maintaining a chain of custody for digital evidence is crucial to document every step of how the evidence is collected, stored, analyzed, and preserved. This process ensures the integrity and reliability of the evidence, making it admissible in court.

Question 44: Which strategy is MOST effective in ensuring data recovery in the event of a catastrophic failure?

(A) Regular penetration testing

(B) Implementing strong encryption algorithms

(C) Offsite backup storage

(D) Deploying antivirus solutions

Correct Answer: (C) Offsite backup storage

Explanation: Offsite backup storage is essential for disaster recovery planning, ensuring that copies of critical data are stored in a geographically separate location. This strategy protects against data loss from catastrophic events, such as natural disasters, fires, or major system failures, enabling organizations to restore data and resume operations.

Question 45: What is the primary function of an intrusion prevention system (IPS)?

(A) To analyze and log traffic for future review

(B) To detect and prevent known threats in real time by analyzing traffic flows

(C) To encrypt traffic between the client and the server

(D) To provide a secure tunnel for data transmission over the internet

Correct Answer: (B) To detect and prevent known threats in real time by analyzing traffic flows

Explanation: An intrusion prevention system (IPS) is designed to detect and prevent known threats by analyzing network traffic in real time. It can take immediate action, such as blocking traffic or alerting administrators, to prevent potential security breaches.

Question 46: Which phase of the incident response process involves actions taken to repair and restore systems or data affected by a cybersecurity incident?

(A) Identification

(B) Containment

(C) Eradication

(D) Recovery

Correct Answer: (D) Recovery

Explanation: The recovery phase of the incident response process involves actions to repair and restore systems or data that have been compromised or affected by a cybersecurity incident. This phase ensures that services are brought back to operational status and any exploited vulnerabilities are addressed to prevent future incidents.

Question 47: In cybersecurity, what is the primary purpose of a vulnerability assessment?

(A) To physically secure the organization's premises

(B) To identify, quantify, and prioritize vulnerabilities in a system

(C) To monitor network traffic for malicious activity

(D) To test the effectiveness of organizational security policies

Correct Answer: (B) To identify, quantify, and prioritize vulnerabilities in a system

Explanation: A vulnerability assessment is a process that identifies, quantifies, and prioritizes vulnerabilities in a system. It aims to uncover security flaws and provide the necessary information to mitigate risks before an attacker can exploit the weaknesses, thereby enhancing the organization's security posture.

Question 48: Before deploying a new application, a large e-commerce company aims to identify and fix any code vulnerabilities. Which method should they use?

(A) Runtime application self-protection (RASP)

(B) Live application penetration testing

(C) Static code analysis

(D) User acceptance testing (UAT)

Correct Answer: (C) Static code analysis

Explanation: Static code analysis, which examines the application's source code for vulnerabilities without executing the program, is the most suitable method for identifying potential security issues before deployment. This preemptive approach helps ensure the application is secure by design.

Question 49: Jenny wants to ensure each asset in her organization has a defined owner. What's the most effective strategy?

(A) Utilize an automated discovery tool and assign assets by location

(B) Assign department heads as default asset owners

(C) Require manual asset claims in audits

(D) Implement an Asset Management System with defined ownership

Correct Answer: (D) Implement an Asset Management System with defined ownership

Explanation: An Asset Management System that logs assets with defined ownership as they're procured or assigned is the most effective way to ensure clear responsibility for asset security and maintenance. This systematic approach ensures accountability and facilitates asset tracking throughout its lifecycle.

Question 50: Following an audit, a company needs to harden its network switches against unauthorized access. What's the BEST approach?

(A) Set up port mirroring

(B) Disable unused ports

(C) Implement load balancing

(D) Increase MAC address table size

Correct Answer: (B) Disable unused ports

Explanation: Disabling unused switch ports is a fundamental network hardening technique, effectively reducing the attack surface by limiting unauthorized access points. This proactive measure enhances network security by minimizing potential vulnerabilities.

Question 51: XenonTech's security team is tasked with monitoring a new web application for vulnerabilities during runtime. Which technique is most appropriate?

(A) Static Analysis

(B) Fuzz Testing

(C) Whitebox Testing

(D) Dynamic Analysis

Correct Answer: (D) Dynamic Analysis

Explanation: Dynamic analysis, which involves evaluating the application's behavior during execution, is ideal for uncovering vulnerabilities that might not be evident in the code itself. This approach allows the team to observe real-time application responses and identify potential security issues.

Question 52: XenonTech seeks real-time updates on emerging threats. What's the BEST source for this information?

(A) Internal vulnerability scanners

(B) Manual penetration tests

(C) OSINT threat feeds

(D) Firewall logs

Correct Answer: (C) OSINT threat feeds

Explanation: Subscribing to an OSINT (Open Source Intelligence) threat feed is the most effective way to stay informed about real-time, evolving threats and vulnerabilities relevant to their industry, offering continuously updated insights from publicly available sources.

Question 53: Prior to finalizing a purchase, a medium-sized enterprise evaluates devices from a cost-effective vendor. What should be their main concern?

(A) Warranty length

(B) Device aesthetics

(C) Compliance with security standards

(D) IT staff training needs

Correct Answer: (C) Compliance with security standards

Explanation: The primary consideration should be the vendor's adherence to industry security standards and practices. Ensuring devices meet established security criteria is crucial for maintaining the organization's security posture and preventing potential vulnerabilities.

Question 54: To understand CyberTech Inc.'s network layout, what activity will enumerate the active devices and their roles?

(A) Vulnerability Scanning

(B) Intrusion Detection

(C) Network Enumeration

(D) Penetration Testing

Correct Answer: (C) Network Enumeration

Explanation: Network enumeration is a process that identifies and categorizes the devices on a network, such as servers, workstations, and network infrastructure devices. It provides a comprehensive view of the network's structure and active components.

Question 55: For secure initial configuration of new routers, what step is paramount?

(A) Enabling DHCP for dynamic IP management

(B) Changing default admin credentials

(C) Updating to the latest firmware for new features

(D) Customizing LED indicators for identification

Correct Answer: (B) Changing default admin credentials.

Explanation: Changing the default administrative credentials on new routers is critical for security. Routers often come with well-known default usernames and passwords, making them vulnerable to unauthorized access if these defaults are not updated.

Question 56: What is the primary objective of implementing a Data Loss Prevention (DLP) system in an organization?

(A) To monitor and protect sensitive data from unauthorized access

(B) To enhance the speed of data transmission within the network

(C) To provide a backup solution for critical data

(D) To detect and mitigate network performance issues

Correct Answer: (A) To monitor and protect sensitive data from unauthorized access

Explanation: The primary objective of a Data Loss Prevention (DLP) system is to monitor, detect, and protect sensitive data across an organization's network and endpoints from unauthorized access or exfiltration, ensuring data privacy and compliance with data protection regulations.

Question 57: What is the primary purpose of conducting a risk assessment in an organization's security program management?

(A) To fulfill insurance requirements

(B) To identify and quantify risks to the organization’s assets and determine appropriate ways to mitigate them

(C) To ensure compliance with all software licenses

(D) To prepare for annual financial audits

Correct Answer: (B) To identify and quantify risks to the organization’s assets and determine appropriate ways to mitigate them.

Explanation: The primary purpose of conducting a risk assessment within an organization's security program is to systematically identify, quantify, and prioritize the risks to the organization's information assets. This process involves evaluating the potential impact of various threats and vulnerabilities, with the goal of implementing appropriate measures to mitigate those risks, thereby enhancing the organization's overall security posture.

Question 58: What role does a Security Policy play in an organization's security program?

(A) It provides detailed technical instructions for configuring network equipment.

(B) It outlines acceptable use of organization's resources and expected behaviors from employees.

(C) It serves as a legal contract between the organization and its customers.

(D) It is a formal document that specifies who has administrative rights on the network.

Correct Answer: (B) It outlines acceptable use of organization's resources and expected behaviors from employees.

Explanation: A Security Policy is a critical component of an organization's security program, providing a formal set of rules and guidelines that outline the acceptable use of the organization's resources and the expected behaviors of its employees and users. It establishes the framework for maintaining a secure environment by defining the scope of security measures, responsibilities, and procedures to protect the organization's assets.

Question 59: Why is it important for an organization to have a Business Continuity Plan (BCP)?

(A) To ensure all employees know their daily tasks

(B) To facilitate rapid recovery and continuation of operations after a significant disruption

(C) To monitor employee activities

(D) To comply with external marketing standards

Correct Answer: (B) To facilitate rapid recovery and continuation of operations after a significant disruption.

Explanation: A Business Continuity Plan (BCP) is essential for any organization as it provides a proactive plan for ensuring that critical business functions can continue during and after a significant disruption, such as a natural disaster, cyberattack, or other crises. The BCP outlines procedures and instructions an organization must follow in the face of such

disasters, focusing on the rapid recovery and continuation of operations to minimize the impact on business operations.

Question 60: How does implementing an Incident Response Plan (IRP) benefit an organization?

(A) It eliminates the need for cybersecurity insurance.

(B) It ensures that no security incidents will occur.

(C) It provides a predefined set of procedures to follow in the event of a security incident.

(D) It automatically mitigates all vulnerabilities in the organization's network.

Correct Answer: (C) It provides a predefined set of procedures to follow in the event of a security incident.

Explanation: An Incident Response Plan (IRP) benefits an organization by providing a structured approach for responding to and managing the aftermath of security incidents. The IRP contains predefined procedures, roles, and responsibilities, which helps to ensure a coordinated and effective response to incidents, thereby minimizing the impact on the organization's operations and reputation.

Question 61: What is the significance of Security Awareness Training within an organization?

(A) It is only necessary for IT staff and security personnel.

(B) It educates employees about the organization's security policy and their role in maintaining security.

(C) It qualifies employees to perform security audits.

(D) It is a one-time requirement during employee onboarding.

Correct Answer: (B) It educates employees about the organization's security policy and their role in maintaining security.

Explanation: Security Awareness Training is significant because it educates all employees, not just IT staff, about the organization's security policies, procedures, and the critical role they play in maintaining security.

Regular training helps to ensure that employees are aware of potential security threats, how to avoid them, and what actions to take in the event of a security incident, thereby enhancing the overall security culture of the organization.

Question 62: What is the primary goal of a Third-Party Risk Management (TPRM) program?

(A) To ensure third parties have faster access to the organization's data

(B) To manage risks associated with outsourcing services and products from third-party vendors

(C) To reduce costs associated with third-party services

(D) To transfer all security risks to third-party vendors

Correct Answer: (B) To manage risks associated with outsourcing services and products from third-party vendors

Explanation: The primary goal of a Third-Party Risk Management (TPRM) program is to identify, assess, monitor, and control the risks associated with outsourcing services and products to third-party vendors. This involves evaluating the security practices of vendors to ensure they meet the organization's standards, thereby protecting the organization from potential security breaches or data leaks originating from third-party sources.

Question 63: Why is it crucial for an organization to conduct regular security audits?

(A) To check the efficiency of the IT department

(B) To evaluate the organization's compliance with its security policies and relevant regulations

(C) To allocate budget for social events

(D) To assess the performance of individual employees

Correct Answer: (B) To evaluate the organization's compliance with its security policies and relevant regulations.

Explanation: Regular security audits are crucial for evaluating an organization's adherence to its internal security policies and any applicable legal and regulatory requirements. These audits help identify gaps in the organization's security posture, assess the effectiveness of implemented security measures, and recommend improvements to ensure the organization maintains a robust defense against cyber threats.

Question 64: What is the purpose of a Security Operations Center (SOC) in an organization?

(A) To serve as a call center for customer service inquiries

(B) To manage the organization's social media accounts

(C) To provide continuous monitoring and analysis of security alerts and incidents

(D) To handle the organization’s financial transactions

Correct Answer: (C) To provide continuous monitoring and analysis of security alerts and incidents

Explanation: A Security Operations Center (SOC) is dedicated to providing continuous monitoring and analysis of an organization's security posture. It is responsible for detecting, analyzing, and responding to cybersecurity incidents using a combination of technology solutions and a strong set of processes. The SOC plays a vital role in the organization's overall security strategy by ensuring potential security threats are identified and mitigated promptly.

Question 65: In security program management, what is the role of a Change Management process?

(A) To document daily activities of the security team

(B) To ensure that changes to the IT infrastructure are performed in a controlled and secure manner

(C) To change the organization's security policies annually

(D) To manage changes in employee roles and responsibilities

Correct Answer: (B) To ensure that changes to the IT infrastructure are performed in a controlled and secure manner

Explanation: The Change Management process in security program management ensures that all changes to the organization's IT infrastructure, whether they are hardware, software, network configurations, or system updates, are executed in a controlled, systematic, and secure manner. This process helps to minimize potential disruptions to services and reduces the risk of introducing new vulnerabilities into the system.

Question 66: How does a vulnerability management program benefit an organization's security posture?

(A) By ensuring all software is proprietary

(B) By facilitating the rapid development of new applications

(C) By systematically identifying, assessing, and mitigating vulnerabilities

(D) By eliminating the need for security policies

Correct Answer: (C) By systematically identifying, assessing, and mitigating vulnerabilities.

Explanation: A vulnerability management program plays a critical role in strengthening an organization's security posture by systematically identifying, assessing, and mitigating vulnerabilities within its systems and networks. This ongoing process involves regular scanning for vulnerabilities, prioritization based on risk, and the implementation of appropriate measures to remediate identified vulnerabilities, thereby reducing the potential attack surface for cyber adversaries.

Question 67: XenonTech and InfoTechSolutions are formalizing their partnership with a set of terms for future transactions. What type of agreement best suits their need to establish foundational business terms?

(A) Memorandum of Understanding (MOU)

(B) Non-Disclosure Agreement (NDA)

(C) Licensing Agreement

(D) Master Service Agreement (MSA)

Correct Answer: (D) Master Service Agreement (MSA)

Explanation: A Master Service Agreement (MSA) is most appropriate for XenonTech and InfoTechSolutions as it outlines the broad framework for all future transactions between the two entities. This agreement will cover essential aspects such as payment terms, delivery protocols, and warranties, setting a standardized set of terms that can be referenced in specific contracts moving forward, thereby streamlining the process for future engagements.

Question 68: InfoTechSolutions's security team is categorizing risks by potential impact levels as part of their new cloud-based project analysis. What type of risk analysis are they conducting?

(A) Quantitative

(B) Statistical

(C) Qualitative

(D) Financial

Correct Answer: (C) Qualitative

Explanation: InfoTechSolutions’s security team is employing a Qualitative risk analysis approach, which assesses and categorizes risks based on non-numeric, descriptive criteria such as Low, Medium, High, and Critical impact levels. This method allows for a subjective but structured evaluation of the potential impacts of identified risks, making it suitable for scenarios where specific numerical data may be unavailable or unnecessary for decision-making.

Question 69: MegaTech Inc. aims to ensure critical applications are restored within 4 hours after any disaster, with a maximum data loss window of 1 hour. Which policy specifically supports this goal?

(A) Data Retention Policy

(B) Incident Response Policy

(C) Disaster Recovery Policy

(D) Password Policy

Correct Answer: (C) Disaster Recovery Policy

Explanation: The Disaster Recovery Policy is specifically designed to address the recovery of IT systems, applications, and data after a catastrophic event. It includes setting Recovery Time Objectives (RTO) for system restoration and Recovery Point Objectives (RPO) for data loss, which are crucial for planning and ensuring business continuity and resilience.

Question 70: In the aftermath of a DDoS attack, the CISO of an e-commerce company stresses the need for a plan encompassing identification to lessons learned. Which policy outlines these stages for managing security incidents?

(A) Change Management Policy

(B) Incident Response Policy

(C) Disaster Recovery Policy

(D) Remote Access Policy

Correct Answer: (B) Incident Response Policy

Explanation: The Incident Response Policy is crucial for defining the procedures and protocols for dealing with security incidents. It typically includes stages such as identification, containment, eradication, recovery, and lessons learned, offering a comprehensive guide to managing and mitigating the impacts of security threats systematically.