



CertsMania

Free Questions for SY0-701

Shared by Dean on Feb 24, 2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



CertsMania

Questions # 1:

A security analyst finds a rogue device during a monthly audit of current endpoint assets that are connected to the network. The corporate network utilizes 802.1X for access control. To be allowed on the network, a device must have a Known hardware address, and a valid user name and password must be entered in a captive portal. The following is the audit report:

>

Which of the following is the most likely way a rogue device was allowed to connect?

Options:

A.

A user performed a MAC cloning attack with a personal device.

B.

A DMCP failure caused an incorrect IP address to be distributed

C.

An administrator bypassed the security controls for testing.

D.

DNS hijacking let an attacker intercept the captive portal traffic.

Answer

A

Explanation

The most likely way a rogue device was able to connect to the network is through a MAC cloning attack. In this attack, a personal device copies the MAC address of an authorized device, bypassing the 802.1X access control that relies on known hardware addresses for network access. The matching MAC addresses in the audit report suggest that this technique was used to gain unauthorized network access.

References =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on Network Security and MAC Address Spoofing.

Questions # 2:

A Chief Information Officer wants to ensure that network devices cannot connect to the public internet and the local network to directly perform firmware updates. The IT team must manually perform the update process by using a portable device. Which of the following architecture types best fits this description?

Options:

A.

Microservices

B.

Air-gapped

C.

Software-defined networking

D.

Serverless



CertsMania

Answer

B

Explanation

The correct answer is Air-gapped because this architecture deliberately isolates systems from external and internal networks to prevent any direct electronic communication. In the Security+ SY0-701 domain of Security Architecture, air-gapped environments are used to achieve the highest level of protection against network-based threats by physically or logically separating critical systems from untrusted networks such as the internet or even the organization's internal network.

In this scenario, the CIO requires that network devices cannot connect to the public internet or the local network for firmware updates, and that updates must be performed manually using a portable device. This is a defining characteristic of an air-gapped architecture. Air-gapped systems rely on controlled, manual transfer methods—such as USB drives or other removable media—to introduce updates, ensuring that malware, remote exploits, and supply-chain-based network attacks cannot reach the isolated systems through traditional network paths.

Option A, Microservices, refers to an application design model where software is built as

loosely coupled services and does not address physical or logical network isolation. Option C, Software-defined networking, focuses on centralized and programmable network control, not network disconnection. Option D, Serverless, is a cloud computing model where infrastructure management is abstracted away from developers and is incompatible with isolated, offline environments.

The SY0-701 study guide highlights air-gapped architectures as common in high-security environments such as industrial control systems, military systems, financial infrastructure, and environments requiring maximum protection against zero-day exploits and remote compromise. While air-gapping introduces operational overhead and update delays, it significantly reduces attack surface and exposure to external threats.

In summary, an architecture that requires manual updates via portable media and prevents any direct network connectivity is best described as air-gapped, making option B the correct answer.

Questions # 3:

A company wants to improve the availability of its application with a solution that requires minimal effort in the event a server needs to be replaced or added. Which of the following would be the best solution to meet these objectives?

Options:

- A.
Load balancing
- B.
Fault tolerance
- C.
Proxy servers
- D.
Replication



CertsMania

Answer

A

Explanation

Detailed Explanation: Load balancing improves application availability by distributing traffic across multiple servers. If one server fails, traffic is automatically routed to other available servers with minimal intervention. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "High Availability Solutions".

Questions # 4:

A new employee accessed an unauthorized website. An investigation found that the employee violated the company's rules. Which of the following did the employee violate?

Options:

A.

MOU

B.

AUP

C.

NDA

D.

MOA

Answer

B

Explanation

An Acceptable Use Policy (AUP) defines what users are permitted and prohibited from doing on an organization's systems, including website access. Accessing unauthorized sites is a common violation of the AUP.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 5.1: "AUPs outline what is and is not acceptable use of organizational resources.", Exam Objectives 5.1: "Explain the importance of organizational security policies, standards, and frameworks.", , , , ,]

Questions # 5:

Which of the following security measures is required when using a cloud-based platform for IoT management?

Options:

- A.
Encrypted connection
- B.
Federated identity
- C.
Firewall
- D.
Single sign-on



CertsMania

Answer

A

Questions # 6:

A security analyst estimates that a small security incident will cost \$10,000 and will occur twice per year. The analyst recommends a budget of \$20,000 for next year. Which of the following does the \$10,000 represent?

Options:

- A.
ARO
- B.
SLE
- C.



CertsMania

- ALE
- D.
- RPO

Answer

B

Explanation



CertsMania

The \$10,000 is the estimated cost per incident (per single occurrence). In quantitative risk analysis, that value is the Single Loss Expectancy (SLE)—the financial impact expected each time a risk event occurs. The Study Guide defines these terms and calculations clearly: “The single loss expectancy (SLE) is the amount of financial damage expected each time a risk materializes.” It also explains how annual impact is derived: “The annualized loss expectancy (ALE) is the amount of damage expected from a risk each year. It is calculated by multiplying the SLE and the ARO.”

Here, the event occurs twice per year, so the Annualized Rate of Occurrence (ARO) is 2.0, and the annual expected loss (ALE) would be $SLE \times ARO = \$10,000 \times 2 = \$20,000$, which matches the recommended budget. That confirms \$10,000 is not ARO (a frequency), not ALE (annual total), and not RPO (a disaster recovery metric about acceptable data loss window).

[References: Quantitative risk terms and formulas (SLE definition; $ALE = SLE \times ARO$) . , ,]

Questions # 7:

A new vulnerability enables a type of malware that allows the unauthorized movement of data from a system. Which of the following would detect this behavior?

Options:

- A.
Implementing encryption
- B.
Monitoring outbound traffic
- C.
Using default settings



CertsMania

D.

Closing all open ports

Answer

B

Explanation



CertsMania

Monitoring outbound traffic is essential for detecting unauthorized data exfiltration from a system. A new vulnerability that allows malware to move data unauthorizedly would typically attempt to send this data out of the network. By monitoring outbound traffic, security tools can detect unusual data transfers, trigger alerts, and help prevent the exfiltration of sensitive information.

References =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Threat Detection and Response.

Questions # 8:

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

Options:

A.

Insurance

B.

Patching

C.

Segmentation

D.

Replacement



CertsMania

Answer

C

Explanation

Segmentation is a technique that divides a network into smaller subnetworks or segments, each with its own security policies and controls. Segmentation can help mitigate network access vulnerabilities in legacy IoT devices by isolating them from other devices and systems, reducing their attack surface and limiting the potential impact of a breach. Segmentation can also improve network performance and efficiency by reducing congestion and traffic. Patching, insurance, and replacement are other possible strategies to deal with network access vulnerabilities, but they may not be feasible or effective in the short term. Patching may not be available or compatible for legacy IoT devices, insurance may not cover the costs or damages of a cyberattack, and replacement may be expensive and time-consuming. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143

Questions # 9:

A systems administrator is working on a solution with the following requirements:

- Provide a secure zone.
- Enforce a company-wide access control policy.
- Reduce the scope of threats.

Which of the following is the systems administrator setting up?

Options:

A.

Zero Trust

B.

AAA

C.

Non-repudiation

D.

CIA



CertsMania

Answer

A

Explanation

Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company-wide access control policy by applying the principle of least privilege and granular segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.

[References:, 5: This source explains the concept and benefits of Zero Trust security and how it differs from traditional security models., 8: This source provides an overview of Zero Trust identity security and how it can help verify the identity and integrity of users and devices., , , , , ,]

Questions # 10:

An accountant is transferring information to a bank over FTP. Which of the following mitigations should the accountant use to protect the confidentiality of the data?

Options:

A.

Tokenization

B.

Data masking

C.

Encryption

D.

Obfuscation



CertsMania

Answer

Questions # 11:

Which of the following technologies can achieve microsegmentation?

Options:

A.

Next-generation firewalls

B.

Software-defined networking

C.

Embedded systems

D.

Air-gapped

Answer

B

Explanation

Software-defined networking (SDN) enables microsegmentation by allowing administrators to create fine-grained, dynamic network segments at the software layer independent of physical network topology. This capability isolates workloads and controls traffic flows between segments, enhancing security within data centers and cloud environments.

Next-generation firewalls (A) provide advanced filtering and inspection but do not inherently deliver the granular segmentation flexibility of SDN. Embedded systems (C) and air-gapped systems (D) refer to specific hardware or physical isolation techniques but do not implement microsegmentation as a network control method.

The concept of microsegmentation through SDN is detailed in the Security Architecture domain of the SY0-701 exam [6:Chapter 3+CompTIA Security+ Study Guide].

Questions # 12:

Which of the following should a security operations center use to improve its incident response procedure?

Options:

A.

Playbooks

B.

Frameworks

C.

Baselines

D.

Benchmarks



CertsMania

Answer

A

Explanation

A playbook is a documented set of procedures that outlines the step-by-step response to specific types of cybersecurity incidents. Security Operations Centers (SOCs) use playbooks to improve consistency, efficiency, and accuracy during incident response. Playbooks help ensure that the correct procedures are followed based on the type of incident, ensuring swift and effective remediation.

Frameworks provide general guidelines for implementing security but are not specific enough for incident response procedures.

Baselines represent normal system behavior and are used for anomaly detection, not incident response guidance.

Benchmarks are performance standards and are not directly related to incident response.

Questions # 13:

Which of the following agreements defines response time, escalation, and performance

metrics?

Options:

A.

BPA

B.

MOA

C.

NDA

D.

SLA



CertsMania

Answer

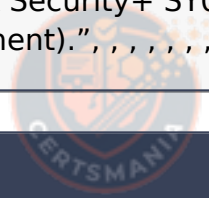
D

Explanation

An SLA (D) or Service Level Agreement is a formal contract that defines performance standards, including response times, escalation procedures, uptime guarantees, and other service-related metrics.

This is referenced in Domain 5.2: Explain the importance of managing third-party risk under "Agreements (e.g., SLA, NDA, MOU/MOA, BPA)."

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 5.2 - "Agreements: SLA (service-level agreement).", , , , , ,]



CertsMania

Questions # 14:

The help desk receives multiple calls that machines with an outdated OS version are running slowly. Several users are seeing virus detection alerts. Which of the following mitigation techniques should be reviewed first?

Options:

A.

Patching

B.

Segmentation

C.

Monitoring

D.

Isolation



CertsMania

Answer

A

Explanation

The best first step is to review patching (A). Outdated OS versions often contain vulnerabilities that can be exploited by malware. Ensuring systems are up-to-date is a foundational cybersecurity practice.

This is highlighted in Domain 2.1: Given a scenario, analyze indicators of malicious activity and Domain 2.2, emphasizing the importance of “Patching” as part of system hardening and mitigation strategy.

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.2 - “Mitigation techniques: Patching.”, , , , , , ,]

Questions # 15:

A security analyst is evaluating a SaaS application that the human resources department would like to implement. The analyst requests a SOC 2 report from the SaaS vendor. Which of the following processes is the analyst most likely conducting?

Options:

A.

Internal audit

B.

Penetration testing

C.

Attestation

D.

Due diligence

Answer

D



CertsMania

Questions # 16:

Which of the following is the final step of the modern response process?

Options:

A.

Lessons learned

B.

Eradication

C.

Containment

D.

Recovery



CertsMania

Answer

A

Explanation

The final step in the incident response process is "Lessons learned." This step involves reviewing and analyzing the incident to understand what happened, how it was handled, and what could be improved. The goal is to improve future response efforts and prevent similar incidents from occurring. It's essential for refining the incident response plan and enhancing overall security posture.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of incident response and recovery.

Questions # 17:

Which of the following can be used to compromise a system that is running an RTOS?

Options:

A.

Cross-site scripting

B.

Memory injection

C.

Replay attack

D.

Ransomware

Answer

B

Questions # 18:

Which of the following is a feature of a next-generation SIEM system?

Options:

A.

Virus signatures

B.

Automated response actions

C.

Security agent deployment

D.

Vulnerability scanning

Answer

B



CertsMania

Questions # 19:

A penetration tester was able to gain unauthorized access to a hypervisor platform. Which of the following vulnerabilities was most likely exploited?

Options:

A.

Cross-site scripting

B.

SQL injection

C.

Race condition

D.

VM escape



CertsMania

Answer

D

Explanation

VM escape is a vulnerability where an attacker breaks out of a virtual machine guest environment to access the host hypervisor, gaining control over other guests or the host system itself.

Cross-site scripting (A) and SQL injection (B) are application-layer attacks. Race condition

(C) is a timing-related vulnerability.

VM escape is a critical threat in virtualized environments discussed under Threats and Vulnerabilities in SY0-701[6:Chapter 2†CompTIA Security+ Study Guide].

Questions # 20:

Which of the following is the best reason to perform a tabletop exercise?

Options:

A.

To address audit findings

B.

To collect remediation response times

C.

To update the IRP

D.

To calculate the ROI

Answer

C

Explanation

A tabletop exercise simulates incident scenarios to test and validate the effectiveness of an organization's Incident Response Plan (IRP), identifying gaps and areas needing updates. It promotes team readiness without disrupting operations.

Addressing audit findings (A), collecting remediation times (B), and calculating ROI (D) are separate activities and not the primary purpose of tabletop exercises.

This practice is an integral part of Security Operations and Incident Response training in SY0-701[6:Chapter 14†CompTIA Security+ Study Guide].

Questions # 21:

An organization implemented cloud-managed IP cameras to monitor building entry points and sensitive areas. The service provider enables direct TCP/IP connection to stream live video footage from each camera. The organization wants to ensure this stream is encrypted and authenticated. Which of the following protocols should be implemented to best meet this objective?

Options:

A.

SSH

B.

SRTP

C.

S/MIME

D.

PPTP



CertsMania

Answer

B

Explanation

Secure Real-Time Transport Protocol (SRTP) is a security protocol used to encrypt and authenticate the streaming of audio and video over IP networks. It ensures that the video streams from the IP cameras are both encrypted to prevent unauthorized access and authenticated to verify the integrity of the stream, making it the ideal choice for securing video surveillance.

[References:, CompTIA Security+ SY0-701 Course Content: Domain 3: Security Architecture, which includes secure communication protocols like SRTP for protecting data in transit., , , , , ,]

Questions # 22:

A systems administrator wants to implement a backup solution. The solution needs to allow recovery of the entire system, including the operating system, in case of a disaster. Which of the following backup types should the administrator consider?

Options:

A.

Incremental

B.

Storage area network

C.

Differential

D.

Image



CertsMania

Answer

D

Explanation

An image backup, also known as a full system backup, captures the entire contents of a system, including the operating system, applications, settings, and all data. This type of backup allows for a complete recovery of the system in case of a disaster, as it includes everything needed to restore the system to its previous state. This makes it the ideal choice for a systems administrator who needs to ensure the ability to recover the entire system, including the OS.

References = CompTIA Security+ SY0-701 study materials, domain on Security Operations

Questions # 23:

The management team wants to assess the cybersecurity team's readiness to respond to a threat scenario. Which of the following will adequately assess and formalize a response within a short time?

Options:

A.

Send a message to all IT managers and request formal action plans.

B.

Create a bug bounty program and assess the findings.

C.

Execute a tabletop exercise and document the performance results.

D.

Hire an external consultant to independently assess the cybersecurity processes.

Answer

C

Explanation

A tabletop exercise is the most effective way to quickly assess a cybersecurity team's readiness to respond to a threat scenario. CompTIA Security+ SY0-701 describes tabletop exercises as discussion-based simulations where incident response team members walk through a realistic scenario to evaluate procedures, decision-making, communication, and coordination. These exercises are specifically designed to be conducted in a short timeframe while still providing meaningful insight into preparedness.

Executing a tabletop exercise allows management to observe how the team identifies threats, escalates incidents, assigns roles, and follows the incident response plan. Documenting performance results helps formalize findings, identify gaps, and improve playbooks and procedures without the complexity of a live incident or full-scale simulation.

Option A is informal and does not test real-time decision-making. Option B focuses on vulnerability discovery, not response readiness. Option D can be effective but is time-consuming and not suited for rapid assessment.

Therefore, C: Execute a tabletop exercise and document the performance results is the correct answer.

Questions # 24:

A company is concerned about the theft of client data from decommissioned laptops. Which of the following is the most cost-effective method to decrease this risk?

Options:

A.

Wiping

B.

Recycling

C.

Shredding

D.

Deletion



CertsMania

Answer

A

Explanation

Wiping involves securely erasing data by overwriting the hard drive, ensuring the information is unrecoverable. It is cost-effective compared to physical destruction methods like shredding.

=====

Questions # 25:

Which of the following best describes why the SMS OTP authentication method is more risky to implement than the TOTP method?

Options:

A.

The SMS OTP method requires an end user to have an active mobile telephone service and SIM card.

B.

Generally, SMS OTP codes are valid for up to 15 minutes while the TOTP time frame is 30 to 60 seconds

C.

The SMS OTP is more likely to be intercepted and lead to unauthorized disclosure of the code



CertsMania

than the TOTP method.

D.

The algorithm used to generate an SMS OTP code is weaker than the one used to generate a TOTP code

Answer

C

Explanation



CertsMania

The SMS OTP (One-Time Password) method is more vulnerable to interception compared to TOTP (Time-based One-Time Password) because SMS messages can be intercepted through various attack vectors like SIM swapping or SMS phishing. TOTP, on the other hand, generates codes directly on the device and does not rely on a communication channel like SMS, making it less susceptible to interception.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management.

=====

Questions # 26:

A security report shows that during a two-week test period, 80% of employees unwittingly disclosed their SSO credentials when accessing an external website. The organization purposely created the website to simulate a cost-free password complexity test. Which of the following would best help reduce the number of visits to similar websites in the future?

Options:

A.

Block all outbound traffic from the intranet.

B.

Introduce a campaign to recognize phishing attempts.

C.

Restrict internet access for the employees who disclosed credentials.

D.



CertsMania

Implement a deny list of websites.

Answer

B

Questions # 27:

Which of the following describes the difference between encryption and hashing?

Options:

A.

Encryption protects data in transit, while hashing protects data at rest.

B.

Encryption replaces cleartext with ciphertext, while hashing calculates a checksum.

C.

Encryption ensures data integrity, while hashing ensures data confidentiality.

D.

Encryption uses a public-key exchange, while hashing uses a private key.

Answer

B

Explanation

Encryption is a reversible process that transforms cleartext data into ciphertext to protect confidentiality. It uses cryptographic keys to both encrypt and decrypt data, ensuring that only authorized parties can access the original data.

Hashing, on the other hand, is a one-way function that converts data into a fixed-length hash value or checksum. Hashing is primarily used to verify data integrity by detecting changes, since any modification in the input will produce a different hash output. Unlike encryption, hashing cannot be reversed to obtain the original data.

While encryption can protect data both at rest and in transit, hashing does not protect data confidentiality but supports integrity verification. Public-key exchange is a

cryptographic mechanism within asymmetric encryption but is unrelated to hashing key usage.

This distinction is thoroughly explained in the Cryptography chapter of the SY0-701 syllabus [6:Chapter 7†CompTIA Security+ Study Guide].

Questions # 28:

Which of the following would be the best way to test resiliency in the event of a primary power failure?

Options:

- A.
Parallel processing
- B.
Tabletop exercise
- C.
Simulation testing
- D.
Production failover

Answer

D

Questions # 29:

Which of the following would best prepare a security team for a specific incident response scenario?

Options:

- A.

Situational awareness

B.

Risk assessment

C.

Root cause analysis

D.

Tabletop exercise



CertsMania

Answer

D

Explanation

A Tabletop exercise (D) is a discussion-based simulation of an incident scenario. It allows security teams to walk through procedures, responsibilities, and communications in a low-pressure environment, improving readiness without impacting operations.

It is specifically designed to prepare teams for real-world incident handling.

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 5.4 - "Incident response plans and exercises: Tabletop exercises." , , , , , ,]

Questions # 30:

Which of the following is a use of CVSS?

Options:

A.

To determine the cost associated with patching systems

B.

To identify unused ports and services that should be closed

C.

To analyze code for defects that could be exploited



CertsMania

D.

To prioritize the remediation of vulnerabilities

Answer

D

Explanation



CertsMania

CVSS (Common Vulnerability Scoring System) is used to assign severity scores to security vulnerabilities, allowing organizations to assess risk and prioritize remediation efforts. By using CVSS scores, teams can address the most critical vulnerabilities first, based on the potential impact.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 4.2: "CVSS is used to score the severity of vulnerabilities and prioritize remediation.", Exam Objectives 4.2: "Summarize vulnerability management processes.", , , , , ,]

Questions # 31:

An organization is evaluating the cost of licensing a new solution to prevent ransomware. Which of the following is the most helpful in making this decision?

Options:

A.

ALE

B.

SLE

C.

RTO

D.

ARO



CertsMania

Answer

A

Explanation

ALE (Annualized Loss Expectancy) is the risk management metric most helpful when deciding whether the licensing cost of a ransomware prevention solution is justified. ALE calculates the expected yearly financial loss from a particular threat. It is computed as:

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

SLE (Single Loss Expectancy) estimates the monetary impact of one ransomware incident.

ARO (Annualized Rate of Occurrence) estimates how often the incident is expected to happen each year.

By comparing ALE to the annual licensing cost of the new security solution, the organization can make a financially informed decision based on cost-benefit analysis. If ALE exceeds the solution's cost, the purchase is justified.

RTO (C) relates to recovery time after outages, not cost justification. SLE (B) is only part of the calculation and insufficient alone. ARO (D) shows frequency but not financial impact.

Security+ SY0-701 highlights ALE as the primary metric for evaluating security investments.

Thus, ALE is the key factor in determining whether purchasing ransomware protection is financially beneficial.

Questions # 32:

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

Options:

A.

Federation

B.

Identity proofing

C.

Password complexity

D.

Default password changes

E.

Password manager

F.

Open authentication



CertsMania

Answer

A, C

Explanation

Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations.

Federation relies on a trusted third party that stores the user's credentials and provides them to the requested resources or services without exposing them. Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness. Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 and 312-313 1

Questions # 33:

A legal department must maintain a backup from all devices that have been shredded and recycled by a third party. Which of the following best describes this requirement?

Options:

A.

Data retention

B.

Certification

C.

Sanitation

D.

Destruction

Answer

A



CertsMania

Questions # 34:

The management team notices that new accounts that are set up manually do not always have correct access or permissions.

Which of the following automation techniques should a systems administrator use to streamline account creation?

Options:

A.

Guard rail script

B.

Ticketing workflow

C.

Escalation script

D.

User provisioning script



CertsMania

Answer

D

Explanation

A user provisioning script is an automation technique that uses a predefined set of instructions or commands to create, modify, or delete user accounts and assign appropriate access or permissions. A user provisioning script can help to streamline

account creation by reducing manual errors, ensuring consistency and compliance, and saving time and resources¹².

The other options are not automation techniques that can streamline account creation:

Guard rail script: This is a script that monitors and enforces the security policies and rules on a system or a network. A guard rail script can help to prevent unauthorized or malicious actions, such as changing security settings, accessing restricted resources, or installing unwanted software³.

Ticketing workflow: This is a process that tracks and manages the requests, issues, or incidents that are reported by users or customers. A ticketing workflow can help to improve the communication, collaboration, and resolution of problems, but it does not automate the account creation process⁴.

Escalation script: This is a script that triggers an alert or a notification when a certain condition or threshold is met or exceeded. An escalation script can help to inform the relevant parties or authorities of a critical situation, such as a security breach, a performance degradation, or a service outage.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: User Provisioning - CompTIA Security+ SY0-701 - 5.1, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 1034: CompTIA Security+ SY0-701 Certification Study Guide, page 104. : CompTIA Security+ SY0-701 Certification Study Guide, page 105.

Questions # 35:

A Chief Information Security Officer wants to monitor the company's servers for SQLi attacks and allow for comprehensive investigations if an attack occurs. The company uses SSL decryption to allow traffic monitoring. Which of the following strategies would best accomplish this goal?

Options:

A.

Logging all NetFlow traffic into a SIEM

B.

Deploying network traffic sensors on the same subnet as the servers

C.

Logging endpoint and OS-specific security logs

D.

Enabling full packet capture for traffic entering and exiting the servers

Answer

D

Explanation



CertsMania

Full packet capture is a technique that records all network traffic passing through a device, such as a router or firewall. It allows for detailed analysis and investigation of network events, such as SQLi attacks, by providing the complete content and context of the packets. Full packet capture can help identify the source, destination, payload, and timing of an SQLi attack, as well as the impact on the server and database. Logging NetFlow traffic, network traffic sensors, and endpoint and OS-specific security logs can provide some information about network activity, but they do not capture the full content of the packets, which may limit the scope and depth of the investigation. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 372-373

Questions # 36:

An attacker submits a request containing unexpected characters in an attempt to gain unauthorized access to information within the underlying systems. Which of the following best describes this attack?

Options:

A.

Side loading

B.

Target of evaluation

C.

Resource reuse

D.

SQL injection



CertsMania

Answer

D

Questions # 37:

Various company stakeholders meet to discuss roles and responsibilities in the event of a security breach that would affect offshore offices. Which of the following is this an example of?

Options:

A.

Tabletop exercise

B.

Penetration test

C.

Geographic dispersion

D.

Incident response

Answer

A

Explanation

A tabletop exercise is a discussion-based simulation in which stakeholders review and talk through their roles, responsibilities, and actions in response to a hypothetical incident. This allows participants to evaluate and improve response plans without actual disruption.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 5.6: "Tabletop exercises involve key stakeholders discussing roles, responsibilities, and actions in response to simulated incidents.", Exam Objectives 5.6: "Given a scenario, implement security incident management processes.", , , , , , ,]

Questions # 38:

Since a recent upgrade of a WLAN infrastructure, several mobile users have been unable to access the internet from the lobby. The networking team performs a heat map survey of the building and finds several WAPs in the area. The WAPs are using similar frequencies with high power settings. Which of the following installation considerations should the security team evaluate next?

Options:

- A.
Channel overlap
- B.
Encryption type
- C.
New WLAN deployment
- D.
WAP placement



CertsMania

Answer

A

Explanation

When multiple Wireless Access Points (WAPs) are using similar frequencies with high power settings, it can cause channel overlap, leading to interference and connectivity issues. This is likely the reason why mobile users are unable to access the internet in the lobby. Evaluating and adjusting the channel settings on the WAPs to avoid overlap is crucial to resolving the connectivity problems.

References = CompTIA Security+ SY0-701 study materials, particularly the domain on Wireless and Mobile Security, which covers WLAN deployment considerations.

Questions # 39:

Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

Options:

A.

Risk tolerance

B.

Risk transfer

C.

Risk register

D.

Risk analysis



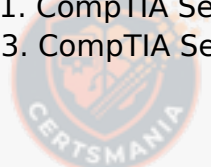
CertsMania

Answer

C

Explanation

A risk register is a document that records and tracks the risks associated with a project, system, or organization. A risk register typically includes information such as the risk description, the risk owner, the risk probability, the risk impact, the risk level, the risk response strategy, and the risk status. A risk register can help identify, assess, prioritize, monitor, and control risks, as well as communicate them to relevant stakeholders. A risk register can also help document the risk tolerance and thresholds of an organization, which are the acceptable levels of risk exposure and the criteria for escalating or mitigating risks. References = CompTIA Security+ Certification Exam Objectives, Domain 5.1: Explain the importance of policies, plans, and procedures related to organizational security. CompTIA Security+ Study Guide (SY0-701), Chapter 5: Governance, Risk, and Compliance, page 211. CompTIA Security+ Certification Guide, Chapter 2: Risk Management, page 33. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 4.



CertsMania

Questions # 40:

During an investigation, a security analyst discovers traffic going out to a command-and-control server. The analyst must find out if any data exfiltration has occurred. Which of the following would best help the analyst determine this?

Options:

A.

Application log

B.

Metadata

C.

Network log

D.

Packet capture



CertsMania

Answer

D

Explanation

To determine whether data exfiltration has occurred, the most effective tool is a packet capture (PCAP). Packet captures allow investigators to see exactly what data left the network, including file contents, payloads, headers, protocols, and destination information. PCAP files provide full-fidelity network evidence, enabling analysts to reconstruct sessions and review exfiltrated content byte-by-byte.

Security+ SY0-701 emphasizes PCAP as the gold standard for forensic network investigations, especially when dealing with:

Malware beaconing

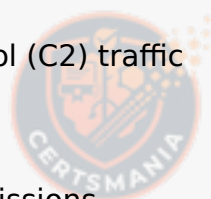
Command-and-control (C2) traffic

Data leakage

Unauthorized transmissions

Network logs (C) provide summaries such as IP addresses, ports, and timestamps but do not show actual data contents. Metadata (B) gives descriptive information (e.g., file size, type) but not transmitted payloads. Application logs (A) show application-level events but do not capture network data.

If the analyst needs to confidently determine if sensitive information was exported to the attacker, only packet capture provides the required depth of visibility.



CertsMania

Questions # 41:

A security analyst identifies an incident in the network. Which of the following incident response activities would the security analyst perform next?

Options:

A.

Containment

B.

Detection

C.

Eradication

D.

Recovery



CertsMania

Answer

A

Explanation

Once an incident is detected, the next step is containment, which involves limiting the scope and impact of the incident to prevent further damage. Containment can be temporary or long-term, isolating affected systems or networks.

Detection (B) is the initial identification phase before containment. Eradication (C) follows containment and involves removing the root cause. Recovery (D) is the final step to restore normal operations.

This workflow is fundamental in the Incident Response lifecycle detailed in Security Operations in SY0-701 [6:Chapter 14+CompTIA Security+ Study Guide].

Questions # 42:

Prior to implementing a design change, the change must go through multiple steps to ensure that it does not cause any security issues. Which of the following is most likely to be one of

those steps?

Options:

A.

Management review

B.

Load testing

C.

Maintenance notifications

D.

Procedure updates



CertsMania

Answer

A

Explanation

Management review is a critical step in the change management process. Before implementing any design change, management reviews help evaluate the potential impact, security implications, and alignment with organizational goals and policies. This review ensures that the change is justified, risks are understood, and proper approvals are obtained.

Load testing is a performance test, maintenance notifications are communication steps, and procedure updates are documentation activities — all important but generally occur after management has approved the change.

The significance of management involvement in change governance is a foundational concept in the Security Program Management and Oversight domain of the SY0-701 exam [6:Chapter 16†CompTIA Security+ Study Guide].

Questions # 43:

A vendor needs to remotely and securely transfer files from one server to another using the command line. Which of the following protocols should be Implemented to allow for this type of access? (Select two).

Options:

A.

SSH

B.

SNMP

C.

RDP

D.

S/MIME

E.

SMTP

F.

SFTP



CertsMania

Answer

A, F

Explanation

Secure Shell (SSH) is a protocol used for secure command-line access to remote systems, while Secure File Transfer Protocol (SFTP) is an extension of SSH used specifically for securely transferring files. Both SSH and SFTP ensure that data is encrypted during transmission, protecting it from interception or tampering.

References =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on Secure Protocols and Encryption.

Questions # 44:

A systems administrator just purchased multiple network devices. Which of the following should the systems administrator perform to prevent attackers from accessing the devices by

using publicly available information?

Options:

A.

Install endpoint protection

B.

Disable ports/protocols

C.

Change default passwords

D.

Remove unnecessary software



CertsMania

Answer

C

Explanation

Changing default passwords is a critical first step after acquiring new devices. Default credentials are widely known and publicly documented, so changing them prevents unauthorized access using this information.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 3.1: "Changing default passwords prevents attackers from exploiting publicly available device information.", Exam Objectives 3.1: "Implement secure network architecture concepts.", , , , ,]



CertsMania

Questions # 45:

An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Select two).

Options:

A.

Application

B.

Authentication

C.

DHCP

D.

Network

E.

Firewall

F.

Database



CertsMania

Answer

C, E

Explanation

To identify the impacted host in a command-and-control (C2) server incident, the following logs should be analyzed:

DHCP logs: These logs record IP address assignments. By reviewing DHCP logs, an organization can determine which host was assigned a specific IP address during the time of the attack.

Firewall logs: Firewall logs will show traffic patterns, including connections to external C2 servers. Analyzing these logs helps to identify the IP address and port numbers of the communicating host.

Application, Authentication, and Database logs are less relevant in this context because they focus on internal processes and authentication events rather than network traffic involved in a C2 attack.

Questions # 46:

Which of the following describes the reason for using an MDM solution to prevent jailbreaking?

Options:

A.

To secure end-of-life devices from incompatible firmware updates

B.

To avoid hypervisor attacks through VM escape

C.

To eliminate buffer overflows at the application layer

D.

To prevent users from changing the OS of mobile devices

Answer

D

Explanation

Mobile Device Management (MDM) solutions can enforce security policies that prevent users from jailbreaking or rooting their devices—that is, from modifying the operating system to remove restrictions and gain unauthorized control. Jailbreaking can introduce significant security risks, so MDM is used to ensure device integrity by preventing users from making these changes.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 3.2: "MDM solutions can be used to prevent users from jailbreaking or rooting devices, maintaining the integrity of the OS.", Exam Objectives 3.2: "Summarize security implications of embedded and specialized systems.", , , , , , , , ,]

Questions # 47:

An organization has a new regulatory requirement to implement corrective controls on a financial system. Which of the following is the most likely reason for the new requirement?

Options:

A.

To defend against insider threats altering banking details

B.

To ensure that errors are not passed to other systems

C.

To allow for business insurance to be purchased

D.

To prevent unauthorized changes to financial data

Answer

D

Explanation

Detailed Explanation:

Corrective controls, such as auditing and versioning, help prevent unauthorized changes to financial data, ensuring data integrity and compliance with regulations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Controls for Financial Systems".

Questions # 48:

Which of the following is a type of vulnerability that may result from outdated algorithms or keys?

Options:

A.

Hash collision

B.

Cryptographic

C.

Buffer overflow

D.

Input validation

Answer

B

Explanation

A cryptographic vulnerability refers to weaknesses caused by the use of outdated or insecure cryptographic algorithms, protocols, or keys. These vulnerabilities make it easier for attackers to compromise encrypted data or communications. Use of deprecated ciphers or insufficient key lengths are typical examples.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 2.3: "Cryptographic vulnerabilities arise from the use of weak or outdated cryptographic algorithms or keys.", Exam Objectives 2.3: "Analyze potential indicators associated with network attacks.", , , , , ,]

Questions # 49:

A company decides to purchase an insurance policy. Which of the following risk management strategies is this company implementing?

Options:

A.

Mitigate

B.

Accept

C.

Avoid

D.

Transfer



CertsMania

Answer

D

Explanation

Purchasing insurance is a classic example of risk transfer, where financial risk associated

with potential losses is shifted to a third party (the insurer). This strategy does not eliminate the risk but moves the financial burden.

Mitigation (A) reduces risk impact or likelihood through controls, acceptance (B) involves acknowledging the risk without action, and avoidance (C) eliminates the risk by not engaging in the activity.

Risk transfer is a fundamental concept taught in the Risk Management domain of SY0-701 [6:Chapter 17†CompTIA Security+ Study Guide].

Questions # 50:

During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers. Which of the following describes an attack method that relates to printing centers?

Options:

A.

Whaling

B.

Credential harvesting

C.

Prepending

D.

Dumpster diving

Answer

D

Explanation

Dumpster diving is an attack method where attackers search through physical waste, such as discarded documents and printouts, to find sensitive information that has not been properly disposed of. In the context of printing centers, this could involve attackers retrieving printed documents containing confidential data that were improperly discarded without shredding or other secure disposal methods. This emphasizes the importance of

proper disposal and physical security measures in cyber hygiene practices.

References =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Physical Security and Cyber Hygiene

Questions # 51:

Attackers created a new domain name that looks similar to a popular file-sharing website. Which of the following threat vectors is being used?

Options:

A.

Watering-hole attack

B.

Brand impersonation

C.

Phishing

D.

Typosquatting

Answer

D

Explanation

Comprehensive and Detailed Explanation From Exact Extract:

The scenario describes attackers registering a similar-looking domain to trick users into visiting a malicious site. This matches the definition of typosquatting, also known as URL hijacking or domain spoofing. Typosquatting relies on users mistyping legitimate URLs or failing to notice slight visual differences (e.g., “dropbx.com” instead of “dropbox.com”). Attackers use these domains to distribute malware, steal credentials, or redirect users to phishing pages.

Watering-hole attacks (A) infect legitimate websites frequented by a specific target group, which does not match this scenario. Brand impersonation (B) involves mimicking a company's identity—often combined with email phishing—but the question specifically mentions creating a similar-looking domain, which is characteristic of typosquatting. Phishing (C) may use these malicious domains, but phishing is a broader social-engineering attack, whereas typosquatting precisely describes the domain manipulation technique.

Security+ SY0-701 emphasizes typosquatting under Social Engineering & Web-based Threats, highlighting how attackers exploit user errors to redirect traffic to malicious destinations. Reducing this risk involves user training, DNS filtering, domain monitoring, and certificate validation.

Questions # 52:

An organization issued new laptops to all employees and wants to provide web filtering both in and out of the office without configuring additional access to the network. Which of the following types of web filtering should a systems administrator configure?

Options:

A.

Agent-based

B.

Centralized proxy

C.

URL scanning

D.

Content categorization



CertsMania

Answer

A

Questions # 53:

Which of the following data recovery strategies will result in a quick recovery at low cost?

Options:

A.

Hot

B.

Cold

C.

Manual

D.

Warm



CertsMania

Answer

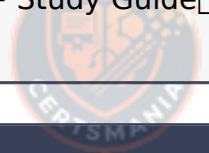
D

Explanation

A warm site offers a compromise between cost and recovery speed. It includes hardware and network infrastructure partially configured, allowing quicker recovery than a cold site but at lower cost than a hot site.

Hot sites (A) enable rapid recovery but at high cost. Cold sites (B) are low cost but slow to recover. Manual (C) refers to manual processes, typically slower.

Warm sites balance recovery time and cost in disaster recovery planning [6:Chapter 9] CompTIA Security+ Study Guide [1].



CertsMania

Questions # 54:

An administrator is reviewing a single server's security logs and discovers the following;

Which of the following best describes the action captured in this log file?

Options:

A.

Brute-force attack

B.

Privilege escalation

C.

Failed password audit

D.

Forgotten password by the user



CertsMania

Answer

A

Explanation

A brute-force attack is a type of attack that involves systematically trying all possible combinations of passwords or keys until the correct one is found. The log file shows multiple failed login attempts in a short amount of time, which is a characteristic of a brute-force attack. The attacker is trying to guess the password of the Administrator account on the server. The log file also shows the event ID 4625, which indicates a failed logon attempt, and the status code 0xC000006A, which means the user name is correct but the password is wrong. These are indicators of compromise (IoC) that suggest a brute-force attack is taking place. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 and 223 1

Questions # 55:

Which of the following explains how regular patching helps mitigate risks when securing an enterprise environment?

Options:

A.

It improves server performance by reducing software bugs.

B.

It addresses known software vulnerabilities before they are exploited.

C.

It eliminates the need for firewalls and intrusion detection.

D.

It removes the need for antivirus tools.

Answer

B

Explanation



CertsMania

The correct answer is B because regular patching directly reduces security risk by remediating known vulnerabilities before attackers can exploit them. Within the Security+ SY0-701 objectives, patch management is a foundational component of vulnerability management and secure operations. Vendors routinely release patches to fix security flaws that have already been identified, documented, and, in many cases, actively targeted by threat actors.

Attackers frequently scan enterprise environments for systems that are missing patches related to publicly disclosed vulnerabilities. Once a vulnerability is known, exploit code often becomes widely available, dramatically increasing the likelihood of compromise. Regular patching shortens the “window of exposure,” which is the time between vulnerability disclosure and remediation. By applying patches promptly, organizations significantly reduce the attack surface and limit opportunities for exploitation.

Option A is incorrect because while patches may incidentally improve stability or performance, that is not their primary security purpose. Option C is incorrect because patching does not replace other security controls; firewalls and intrusion detection systems remain essential for layered defense. Option D is also incorrect because antivirus tools serve a different role, such as detecting and responding to malware, and cannot be replaced by patching alone.

The SY0-701 study guide emphasizes that effective patch management requires structured processes, including testing, maintenance windows, rollback planning, and prioritization based on risk and asset criticality. Patching is classified as a preventive technical control, stopping attacks before they occur rather than reacting after compromise.

In summary, regular patching mitigates enterprise risk by proactively addressing known software vulnerabilities before they can be exploited. This makes it one of the most effective and widely emphasized security practices in the Security+ SY0-701 exam and in real-world security operations.

Questions # 56:

A security administrator would like to protect data on employees' laptops. Which of the following encryption techniques should the security administrator use?

Options:

A.

Partition

B.

Asymmetric

C.

Full disk

D.

Database



CertsMania

Answer

C

Explanation

Full disk encryption (FDE) is a technique that encrypts all the data on a hard drive, including the operating system, applications, and files. FDE protects the data from unauthorized access in case the laptop is lost, stolen, or disposed of without proper sanitization. FDE requires the user to enter a password, a PIN, a smart card, or a biometric factor to unlock the drive and boot the system. FDE can be implemented by using software solutions, such as BitLocker, FileVault, or VeraCrypt, or by using hardware solutions, such as self-encrypting drives (SEDs) or TrustedPlatform Modules (TPMs). FDE is a recommended encryption technique for laptops and other mobile devices that store sensitive data.

Partition encryption is a technique that encrypts only a specific partition or volume on a hard drive, leaving the rest of the drive unencrypted. Partition encryption is less secure than FDE, as it does not protect the entire drive and may leave traces of data on unencrypted areas. Partition encryption is also less convenient than FDE, as it requires the user to mount and unmount the encrypted partition manually.

Asymmetric encryption is a technique that uses a pair of keys, one public and one private, to encrypt and decrypt data. Asymmetric encryption is mainly used for securing communication, such as email, web, or VPN, rather than for encrypting data at rest. Asymmetric encryption is also slower and more computationally intensive than symmetric encryption, which is the type of encryption used by FDE and partition encryption.

Database encryption is a technique that encrypts data stored in a database, such as tables, columns, rows, or cells. Database encryption can be done at the application level, the database level, or the file system level. Database encryption is useful for protecting data from unauthorized access by database administrators, hackers, or malware, but it does not protect the data from physical theft or loss of the device that hosts the database.

References = Data Encryption - CompTIA Security+ SY0-401: 4.4, CompTIA Security+ Cheat Sheet and PDF | Zero To Mastery, CompTIA Security+ SY0-601 Certification Course - Cybr, Application Hardening - SY0-601 CompTIA Security+ : 3.2.

Questions # 57:

Which vulnerability is most likely mitigated by setting up an MDM platform?

Options:

A.

TPM

B.

Buffer overflow

C.

Jailbreaking

D.

SQL injection

Answer

C

Explanation

Mobile Device Management (MDM) platforms enforce security policies on mobile devices, including preventing or detecting jailbreaking, which is the act of removing manufacturer restrictions on devices. Jailbroken devices bypass security protections, allow installation of unauthorized apps, expose system files, and greatly increase risk.

Security+ SY0-701 identifies MDM as a key defense for mobile ecosystems, providing controls such as:

Jailbreak/root detection

Remote wipe

App allow/deny lists

Configuration enforcement

Encryption enforcement

TPM (A) is hardware-based protection unrelated to MDM. Buffer overflow (B) and SQL injection (D) are software coding vulnerabilities not affected by mobile device policy enforcement.

Thus, the correct answer is C: Jailbreaking.

Questions # 58:

During a SQL update of a database, a temporary field used as part of the update sequence was modified by an attacker before the update completed in order to allow access to the system. Which of the following best describes this type of vulnerability?

Options:

A.

Race condition

B.

Memory injection

C.

Malicious update

D.

Side loading

Answer

A

Explanation

A race condition occurs when two or more processes attempt to access and modify a shared resource simultaneously, leading to unintended behavior. In this scenario, the attacker was able to modify a temporary field before the SQL update completed, indicating a time-of-check to time-of-use (TOCTOU) vulnerability, which is a type of race condition.

Memory injection (B) refers to inserting malicious code into a running process's memory, but that is not what is happening here.

Malicious update (C) is too broad and does not specifically describe this scenario.

Side loading (D) is a technique where malicious software is loaded via a trusted application, unrelated to this case.

[Reference: CompTIA Security+ SY0-701 Official Study Guide, Threats, Vulnerabilities, and Mitigations domain., , , , ,]

Questions # 59:

Which of the following are the most important considerations when encrypting data? (Select two).

Options:

A.

Obfuscation

B.

Algorithms

C.

Data masking

D.

Key length

E.

Tokenization

F.

Salting



CertsMania

Answer

B, D

Explanation

When encrypting data, two fundamental drivers of cryptographic strength are the algorithm you choose and the key length you use (which affects brute-force feasibility and overall security margin). The Study Guide emphasizes algorithm selection as a best practice: "First, choose your encryption system wisely... Choose an encryption system with an algorithm in the public domain that has been thoroughly vetted by industry experts." It then highlights key selection/size as another central decision: "You must also select your keys in an appropriate manner. Use a key length that balances your security requirements with performance considerations."

These two choices directly affect whether encryption meaningfully protects confidentiality. By contrast, obfuscation, masking, and tokenization are different data-protection techniques (often used to reduce exposure or de-identify data) rather than core encryption-strength parameters. Salting is primarily associated with strengthening password hashing (defending against rainbow table attacks), not selecting encryption primitives/strength for general data encryption. Therefore, the best two considerations in the context of encryption itself are Algorithms and Key length.

[References: Encryption best practices—select vetted algorithms and appropriate key length ., ., .]

Questions # 60:

Which of the following actions is best performed by ticketing automation to ensure that incidents receive the correct level of attention and response?

Options:

A.

Notification

B.

Creation

C.

Closure

D.



CertsMania

Answer

D

Explanation

The key phrase is “ensure that incidents receive the correct level of attention and response.” In operations, that aligns most directly with escalation—moving high-severity or time-sensitive incidents to the right people/teams quickly and consistently, according to predefined criteria (severity, impacted systems, threat intel enrichment, SLA timers). The Study Guide lists ticketing and escalation explicitly as automation use cases: “Ticket creation: Automation can streamline the ticketing process, enabling immediate creation and routing of issues to the right teams.” and, crucially for this question, “Escalation: In case of a major incident, scripts can automate the escalation process, alerting key personnel quickly.”

While automation can also handle notification and ticket creation, escalation is the control that most directly enforces that the incident gets the proper priority and response path (for example: paging on-call, invoking the IR lead, opening a bridge, and applying “major incident” workflows). Closure is typically less suitable because it often requires validation and human judgment to ensure containment, eradication, and recovery steps are complete.

[References: Automation use cases for ticketing, including escalation for major incidents ., ,]

Questions # 61:

A company is implementing a policy to allow employees to use their personal equipment for work. However, the company wants to ensure that only company-approved applications can be installed. Which of the following addresses this concern?

Options:

A.

MDM

B.

Containerization

C.

DLP

D.

FIM

Answer

A

Explanation



CertsMania

Comprehensive and Detailed In-Depth Explanation:

Mobile Device Management (MDM) is a security solution that allows organizations to enforce policies on employee-owned or company-issued mobile devices. It can restrict the installation of unauthorized applications, ensuring that only company-approved apps are used.

Containerization isolates work applications from personal applications but does not enforce app restrictions.

Data Loss Prevention (DLP) focuses on preventing sensitive data leaks rather than managing app installations.

File Integrity Monitoring (FIM) tracks changes to files and system configurations but does not control app installations.

Therefore, MDM is the best solution for restricting unauthorized applications on personal devices.

Questions # 62:

A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

Options:

A.

Private

B.

Critical

C.

Sensitive

D.

Public

Answer

C

Explanation

Data classification is a process of categorizing data based on its level of sensitivity, value, and impact to the organization if compromised. Data classification helps to determine the appropriate security controls and policies to protect the data from unauthorized access, disclosure, or modification. Different organizations may use different data classification schemes, but a common one is the four-tier model, which consists of the following categories: public, private, sensitive, and critical.

Public data is data that is intended for public access and disclosure, and has no impact to the organization if compromised. Examples of public data include marketing materials, press releases, and public web pages.

Private data is data that is intended for internal use only, and has a low to moderate impact to the organization if compromised. Examples of private data include employee records, financial reports, and internal policies.

Sensitive data is data that is intended for authorized use only, and has a high impact to the organization if compromised. Examples of sensitive data include personal information, health records, and intellectual property.

Critical data is data that is essential for the organization's operations and survival, and has a severe impact to the organization if compromised. Examples of critical data include encryption keys, disaster recovery plans, and system backups.

Patient data is a type of sensitive data, as it contains personal and health information that is protected by law and ethical standards. Patient data should be used only by authorized personnel for legitimate purposes, and should be secured from unauthorized access, disclosure, or modification. Therefore, the systems administrator should use the sensitive data classification to secure patient data.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 90-91; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.5 - Data Classifications, 0:00 - 4:30.

Questions # 63:

A security engineer configured a remote access VPN. The remote access VPN allows end users to connect to the network by using an agent that is installed on the endpoint, which establishes an encrypted tunnel. Which of the following protocols did the engineer most likely implement?

Options:

- A.
GRE
- B.
IPSec
- C.
SD-WAN
- D.
EAP



CertsMania

Answer

B

Questions # 64:

Which security controls is a company implementing by deploying HIPS? (Select two)

Options:

- A.
Directive
- B.
Preventive
- C.



CertsMania

Physical

D.

Corrective

E.

Compensating

F.

Detective



CertsMania

Answer

B, F

Explanation

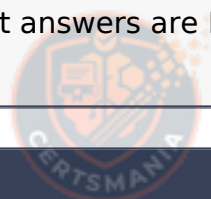
A Host-Based Intrusion Prevention System (HIPS) provides preventive and detective security controls. Security+ SY0-701 explains that:

As a preventive control (B), HIPS actively blocks malicious behavior, stops unauthorized changes, prevents exploit execution, and enforces host-level protection. It prevents malware, intrusions, and unauthorized actions before they occur.

As a detective control (F), HIPS monitors host activity, detects suspicious patterns, logs events, and alerts administrators when threats are observed.

Directive controls (A) involve policy, not technical tools. Physical controls (C) include barriers and locks. Corrective controls (D) restore systems after incidents. Compensating controls (E) are alternatives when primary controls aren't available.

Therefore, the correct answers are B (Preventive) and F (Detective).



CertsMania

Questions # 65:

Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).

Options:

A.

The device has been moved from a production environment to a test environment.

B.

The device is configured to use cleartext passwords.

C.

The device is moved to an isolated segment on the enterprise network.

D.

The device is moved to a different location in the enterprise.

E.

The device's encryption level cannot meet organizational standards.

F.

The device is unable to receive authorized updates.

Answer

E

Explanation

An engineer should recommend the decommissioning of a network device when the device poses a security risk or a compliance violation to the enterprise environment. A device that cannot meet the encryption standards or receive authorized updates is vulnerable to attacks and breaches, and may expose sensitive data or compromise network integrity. Therefore, such a device should be removed from the network and replaced with a more secure and updated one.

References

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, Section 2.2, page 671

CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 2, Question 16, page 512

Questions # 66:

A security analyst is concerned malicious actors are lurking in an environment but has not received any alerts regarding suspicious activity. Which of the following should the analyst conduct to further investigate the presence of these actors?

Options:

A.

Threat hunting

B.

Digital forensics

C.

Vulnerability scanning

D.

E-discovery



CertsMania

Answer

A

Explanation

Threat hunting is a proactive security activity focused on identifying hidden or undetected threats within an environment, even when no alerts or indicators have been triggered. According to CompTIA Security+ SY0-701, threat hunting assumes that attackers may already be present and actively evading traditional security controls such as SIEMs, IDS/IPS, or endpoint protection tools.

Threat hunting involves manually analyzing logs, endpoint telemetry, network traffic, and behavioral patterns to uncover anomalies that automated systems may miss. This aligns directly with the scenario, where the analyst has a suspicion of malicious actors but no alerts confirming activity. Threat hunting helps identify advanced persistent threats (APTs), living-off-the-land techniques, credential misuse, and lateral movement that may not generate immediate alerts.

Digital forensics (B) is typically performed after an incident has been confirmed. Vulnerability scanning (C) identifies weaknesses but does not detect active attackers. E-discovery (D) is a legal process for collecting electronically stored information and is not used for threat detection.

Because the analyst is proactively searching for hidden threats without existing alerts, the correct action is A: Threat hunting.

Questions # 67:

A Chief Security Officer signs off on a request to allow inbound SMB and RDP from the internet to a single VLAN. Which of the following is the most likely explanation for this activity?

Options:

A.

The company built a new file-sharing site.

B.

The organization is preparing for a penetration test.

C.

The security team is integrating with an SASE platform.

D.

The security team created a honeynet.

Answer

D

Explanation

Allowing risky protocols like SMB and RDP from the internet to a controlled VLAN is commonly done to create a honeynet, a deliberately vulnerable network environment used to attract attackers and study their behaviors without risking production systems.

Building a file-sharing site (A) or preparing for a pentest (B) typically wouldn't require exposing SMB and RDP broadly. SASE integration (C) focuses on cloud security access and doesn't involve opening such protocols indiscriminately.

Honeynets are described as a deception technology in the Security Architecture domain [6:Chapter 9+CompTIA Security+ Study Guide].

Questions # 68:

During a recent log review, an analyst found evidence of successful injection attacks. Which of the following will best address this issue?

Options:

A.

Authentication

B.

Secure cookies

C.

Static code analysis

D.

Input validation



CertsMania

Answer

D

Explanation

Comprehensive and Detailed In-Depth Explanation:

Input validation ensures that only properly formatted and expected input is accepted by an application, preventing injection attacks such as SQL injection and command injection. Properly validating and sanitizing user inputs can mitigate these types of attacks.

Authentication (A) helps verify user identity but does not prevent injection attacks.

Secure cookies (B) protect session data but do not stop injection-based exploits.

Static code analysis (C) can help identify vulnerabilities but does not actively prevent injection attacks in real-time.

Implementing strong input validation can prevent malicious code from being executed, reducing the risk of injection attacks.

Questions # 69:

A systems administrator needs to ensure the secure communication of sensitive data within the organization's private cloud. Which of the following is the best choice for the administrator to implement?

Options:

A.

IPSec

B.

SHA-1

C.

RSA

D.

TGT



CertsMania

Answer

A

Questions # 70:

A company must ensure sensitive data at rest is rendered unreadable. Which of the following will the company most likely use?

Options:

A.

Hashing

B.

Tokenization

C.

Encryption

D.

Segmentation



CertsMania

Answer

C

Explanation

Encryption is a method of transforming data in a way that makes it unreadable without a secret key necessary to decrypt the data back into plaintext. Encryption is one of the most common and effective ways to protect data at rest, as it prevents unauthorized access, modification, or theft of the data. Encryption can be applied to different types of data at rest, such as block storage, object storage, databases, archives, and so on. Hashing, tokenization, and segmentation are not methods of rendering data at rest unreadable, but rather of protecting data in other ways. Hashing is a one-way function that generates a fixed-length output, called a hash or digest, from an input, such that the input cannot be recovered from the output. Hashing is used to verify the integrity and authenticity of data, but not to encrypt it. Tokenization is a process that replaces sensitive data with non-sensitive substitutes, called tokens, that have no meaning or value on their own. Tokenization is used to reduce the exposure and compliance scope of sensitive data, but not to encrypt it. Segmentation is a technique that divides a network or a system into smaller, isolated units, called segments, that have different levels of access and security. Segmentation is used to limit the attack surface and contain the impact of a breach, but not to encrypt data at rest. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, pages 77-781; Protecting data at rest - Security Pillar3

Questions # 71:

Which of the following environments utilizes a subset of customer data and is most likely to be used to assess the impacts of major system upgrades and demonstrate system features?

Options:

- A.
Development
- B.
Test
- C.
Production
- D.
Staging



Answer

D

Explanation

A staging environment is a controlled setting that closely mirrors the production environment but uses a subset of customer data. It is used to test major system upgrades, assess their impact, and demonstrate new features before they are rolled out to the live production environment. This ensures that any issues can be identified and addressed in a safe environment before affecting end-users.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of secure system development and testing environments.

Questions # 72:

The security team at a large global company needs to reduce the cost of storing data used for performing investigations. Which of the following types of data should have its retention length reduced?

Options:

A.

Packet capture

B.

Endpoint logs

C.

OS security logs

D.

Vulnerability scan



CertsMania

Answer

A

Explanation

Packet capture data can be very large and may not need to be stored for extended periods compared to other logs essential for security audits.

=====

Questions # 73:

Which of the following can be used to identify potential attacker activities without affecting production servers?

Options:

A.

Honey pot

B.

Video surveillance

C.

Zero Trust

D.

Geofencing

Answer

A

Explanation

A honey pot is a system or a network that is designed to mimic a real production server and attract potential attackers. A honey pot can be used to identify the attacker's methods, techniques, and objectives without affecting the actual production servers. A honey pot can also divert the attacker's attention from the real targets and waste their time and resources¹².

The other options are not effective ways to identify potential attacker activities without affecting production servers:

Video surveillance: This is a physical security technique that uses cameras and monitors to record and observe the activities in a certain area. Video surveillance can help to deter, detect, and investigate physical intrusions, but it does not directly identify the attacker's

activities on the network or the servers³.

Zero Trust: This is a security strategy that assumes that no user, device, or network is trustworthy by default and requires strict verification and validation for every request and transaction. Zero Trust can help to improve the security posture and reduce the attack surface of an organization, but it does not directly identify the attacker's activities on the network or the servers⁴.

Geofencing: This is a security technique that uses geographic location as a criterion to restrict or allow access to data or resources. Geofencing can help to protect the data sovereignty and compliance of an organization, but it does not directly identify the attacker's activities on the network or the servers⁵.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Honeypots and Deception - SY0-601 CompTIA Security+ : 2.1, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 985: CompTIA Security+ SY0-701 Certification Study Guide, page 99.

Questions # 74:

A business needs a recovery site but does not require immediate failover. The business also wants to reduce the workload required to recover from an outage. Which of the following recovery sites is the best option?

Options:

A.

Hot

B.

Cold

C.

Warm

D.

Geographically dispersed



CertsMania

Answer

C

Explanation

A warm site is the best option for a business that does not require immediate failover but wants to reduce the workload required for recovery. A warm site has some pre-installed equipment and data, allowing for quicker recovery than a cold site, but it still requires some setup before becoming fully operational.

Hot sites provide immediate failover but are more expensive and require constant maintenance.

Cold sites require significant time and effort to get up and running after an outage.

Geographically dispersed sites refer to a specific location strategy rather than the readiness of the recovery site.

Questions # 75:

Which of the following architecture models ensures that critical systems are physically isolated from the network to prevent access from users with remote access privileges?

Options:

A.

Segmentation

B.

Virtualized

C.

Air-gapped

D.

Serverless

Answer

C

Explanation

An air-gapped (C) system is completely isolated from unsecured networks (like the internet)

and other systems, preventing any form of remote access. This is often used in highly sensitive environments such as military, nuclear, or critical infrastructure systems.

This is mentioned under Domain 3.4: Given a scenario, apply cybersecurity resilience concepts in the CompTIA Security+ SY0-701 Exam Objectives, specifically under “Isolation (e.g., air-gapped)”.

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.4 – “Cybersecurity resilience: Isolation (e.g., air-gapped).”, , , , , ,]

Questions # 76:

An analyst is reviewing an incident in which a user clicked on a link in a phishing email. Which of the following log sources would the analyst utilize to determine whether the connection was successful?

Options:

A.

Network

B.

System

C.

Application

D.

Authentication

Answer

A

Explanation

To determine whether the connection was successful after a user clicked on a link in a phishing email, the most relevant log source to analyze would be the network logs. These logs would provide information on outbound and inbound traffic, allowing the analyst to see if the user’s system connected to the remote server specified in the phishing link. Network logs can include details such as IP addresses, domains accessed, and the success or failure of connections, which are crucial for understanding the impact of the phishing attempt.

References =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Incident Response.

Questions # 77:

Which of the following hardening techniques must be applied on a container image before deploying it to a production environment? (Select two).

Options:

A.

Remove default applications.

B.

Install a NIPS.

C.

Disable Telnet.

D.

Reconfigure the DNS

E.

Add an SFTP server.

F.

Delete the public certificate.

Answer

A, C

Explanation

Container image hardening best practices include removing default or unnecessary applications (A) to reduce the attack surface and disabling insecure protocols like Telnet (C) to prevent exploitation. Minimizing software components reduces vulnerabilities and

limits potential exploits.

Installing a Network Intrusion Prevention System (NIPS) (B) is a network security measure, not typically embedded in a container image. Reconfiguring DNS (D), adding an SFTP server (E), or deleting public certificates (F) are unrelated or could disrupt container functionality.

These practices are part of securing containerized environments covered under Security Architecture topics in SY0-701 [6:Chapter 10] CompTIA Security+ Study Guide [6].

Questions # 78:

Which of the following allows for the attribution of messages to individuals?

Options:

- A.
Adaptive identity
- B.
Non-repudiation
- C.
Authentication
- D.
Access logs

Answer

B

Explanation

Non-repudiation is the ability to prove that a message or document was sent or signed by a particular person, and that the person cannot deny sending or signing it. Non-repudiation can be achieved by using cryptographic techniques, such as hashing and digital signatures, that can verify the authenticity and integrity of the message or document. Non-repudiation can be useful for legal, financial, or contractual purposes, as it can provide evidence of the origin and content of the message or document. References = Non-repudiation - CompTIA Security+ SY0-701 - 1.2, CompTIA Security+ SY0-301: 6.1 - Non-repudiation, CompTIA Security+ (SY0-701) Certification

Questions # 79:

A security analyst is examining a penetration test report and notices that the tester pivoted to critical internal systems with the same local user ID and password. Which of the following would help prevent this in the future?

Options:

A.

Implement centralized authentication with proper password policies

B.

Add password complexity rules and increase password history limits

C.

Connect the systems to an external authentication server

D.

Limit the ability of user accounts to change passwords

Answer

A

Explanation

Centralized authentication (such as Active Directory or LDAP) combined with proper password policies helps prevent the reuse of the same local credentials across multiple systems, reducing the risk of lateral movement during attacks like credential reuse or pass-the-hash.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 3.1: "Centralized authentication and strong password policies reduce risks associated with local account reuse.", Exam Objectives 3.1: "Implement secure network architecture concepts." , , , , ,]

Questions # 80:

Which of the following is a possible consequence of a VM escape?

Options:

A.

Malicious instructions can be inserted into memory and give the attacker elevated permissions.

B.

An attacker can access the hypervisor and compromise other VMs.

C.

Unencrypted data can be read by a user in a separate environment.

D.

Users can install software that is not on the manufacturer's approved list.

Answer

B

Explanation

Detailed Explanation: A VM escape occurs when an attacker breaks out of a virtual machine's isolation to access the hypervisor. This compromise can allow control of the hypervisor and all other VMs on the host, posing significant security risks. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Virtualization Risks and Mitigation".

Questions # 81:

Which of the following is the most likely benefit of conducting an internal audit?

Options:

A.

Findings are reported to shareholders.

B.

Reports are not formal and can be reassigned.

C.

Control gaps are identified for remediation.

D.

The need for external audits is eliminated.

Answer

C

Explanation

Internal audits are conducted within an organization to independently assess and evaluate the effectiveness of internal controls, policies, and procedures. A key benefit of internal audits is the identification of control gaps or weaknesses that can then be remediated before they lead to security incidents or compliance failures.

Unlike external audits, internal audit findings are primarily for management and internal stakeholders, focusing on improving security posture and operational efficiency. Reports generated are formal and documented to ensure accountability, and internal audits do not replace the need for external audits, which provide independent verification to external parties like regulators or shareholders.

This role of internal audits in identifying deficiencies and driving remediation efforts is emphasized in the Security Program Management and Oversight domain of the SY0-701 exam [7:Chapter 5+CompTIA Security+ Practice Tests].

Questions # 82:

Which of the following can be best used to discover a company's publicly available breach information?

Options:

A.

OSINT

B.

SIEM

C.

CVE

D.

CVSS

Answer

A

Explanation

OSINT (Open Source Intelligence) involves collecting publicly available information, including data breaches, leaked credentials, and other exposed company data found online or on the dark web. OSINT tools can discover if a company's information has been compromised publicly.

SIEM (Security Information and Event Management) monitors internal logs and events but does not collect external breach info. CVE (Common Vulnerabilities and Exposures) is a database of known software vulnerabilities, not breach data. CVSS (Common Vulnerability Scoring System) rates vulnerabilities' severity.

OSINT is a key technique in the Threats and Vulnerabilities domain for external threat intelligence gathering [6:Chapter 2] CompTIA Security+ Study Guide [6].

Questions # 83:

An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

Options:

A.

RDP server

B.

Jump server

C.

Proxy server

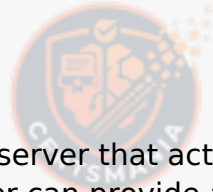
D.

Hypervisor

Answer

B

Explanation



CertsMania

= A jump server is a server that acts as an intermediary between a user and a target system. A jump server can provide an added layer of security by preventing unauthorized access to internal company resources. A user can connect to the jump server using a secure protocol, such as SSH, and then access the target system from the jump server. This way, the target system is isolated from the external network and only accessible through the jump server. A jump server can also enforce security policies, such as authentication, authorization, logging, and auditing, on the user's connection. A jump server is also known as a bastion host or a jump box. References = CompTIA Security+ Certification Exam Objectives, Domain 3.3: Given a scenario, implement secure network architecture concepts. CompTIA Security+ Study Guide (SY0-701), Chapter 3: Network Architecture and Design, page 101. Other Network Appliances - SY0-601 CompTIA Security+ : 3.3, Video 3:03. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 2.

Questions # 84:

Which of the following activities is the first stage in the incident response process?

Options:

A.

Detection

B.

Declaration

C.

Containment

D.

Vacation



CertsMania

Answer

A

Questions # 85:

For which of the following reasons would a systems administrator leverage a 3DES hash from an installer file that is posted on a vendor's website?

Options:

A.

To test the integrity of the file

B.

To validate the authenticity of the file

C.

To activate the license for the file

D.

To calculate the checksum of the file

Answer

A

Questions # 86:

Which of the following is a benefit of an RTO when conducting a business impact analysis?

Options:

A.

It determines the likelihood of an incident and its cost.

B.

It determines the roles and responsibilities for incident responders.

C.

It determines the state that systems should be restored to following an incident.

D.

It determines how long an organization can tolerate downtime after an incident.

Answer

D

Explanation

Recovery Time Objective (RTO) defines the maximum acceptable downtime before business operations must be restored. It helps organizations set expectations for recovery speed and prioritize system restoration accordingly.

A (likelihood of an incident and cost) relates to risk assessment, not RTO.

B (roles and responsibilities) falls under incident response planning, not RTO.

C (state of restored systems) is covered by Recovery Point Objective (RPO), not RTO.

[Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain., , , , , ,]

Questions # 87:

An alert references attacks associated with a zero-day exploit. An analyst places a bastion host in the network to reduce the risk of the exploit. Which of the following types of controls is the analyst implementing?

Options:

A.

Compensating

B.

Detective

C.

Operational

D.

Physical

Answer

A

Explanation



CertsMania

The correct answer is Compensating because a bastion host is being used as an alternative safeguard to reduce risk when a primary control cannot yet be fully implemented. In the context of the Security+ SY0-701 objectives, compensating controls are designed to provide protection when standard preventive controls are not available, effective, or feasible—such as during a zero-day exploit where no vendor patch or permanent fix exists.

A zero-day exploit represents a vulnerability that is actively being exploited before developers or vendors have released a fix. Since patching is not immediately possible, organizations must rely on compensating controls to limit exposure and reduce the likelihood or impact of exploitation. A bastion host is a hardened system placed in a network segment—often in a demilitarized zone (DMZ)—that acts as a controlled access point between untrusted and trusted networks. By routing access through this tightly secured host, the analyst reduces the attack surface and restricts direct access to internal systems that may be vulnerable to the zero-day.

Option B, Detective, is incorrect because detective controls are focused on identifying or alerting on malicious activity after it occurs, such as logging, monitoring, or intrusion detection systems. Option C, Operational, refers to processes and procedures carried out by people, such as incident response or change management, rather than a technical safeguard. Option D, Physical, applies to tangible protections like locks, cameras, or fencing, which are not relevant in this network-based scenario.

The SY0-701 study guide emphasizes the importance of layered security and adaptive risk management. When preventive controls fail or are temporarily unavailable, compensating controls like bastion hosts, network segmentation, and access restrictions allow organizations to maintain security posture and continuity of operations while longer-term solutions are developed.

Questions # 88:

Which of the following is required for an organization to properly manage its restore process in the event of system failure?

Options:

A.

IRP

B.

DRP

C.

RPO

D.

SDLC



CertsMania

Answer

B

Explanation

A disaster recovery plan (DRP) is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. A DRP typically includes the following elements:

A risk assessment that identifies the potential threats and impacts to the organization's critical assets and processes.

A business impact analysis that prioritizes the recovery of the most essential functions and data.

A recovery strategy that defines the roles and responsibilities of the recovery team, the resources and tools needed, and the steps to follow to restore the system.

A testing and maintenance plan that ensures the DRP is updated and validated regularly. A DRP is required for an organization to properly manage its restore process in the event of system failure, as it provides a clear and structured framework for recovering from a disaster and minimizing the downtime and data loss. References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325.

Questions # 89:

A security analyst is reviewing logs and discovers the following:

>

Which of the following should be used to best mitigate this type of attack?

Options:

- A.
Input sanitization
- B.
Secure cookies
- C.
Static code analysis
- D.
Sandboxing



CertsMania

Answer

A

Questions # 90:

An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?

Options:

- A.
Secured zones
- B.
Subject role
- C.
Adaptive identity
- D.



CertsMania

Threat scope reduction

Answer

D

Explanation

The data plane, also known as the forwarding plane, is the part of the network that carries user traffic and data. It is responsible for moving packets from one device to another based on the routing and switching decisions made by the control plane. The data plane is a critical component of the Zero Trust architecture, as it is where most of the attacks and breaches occur. Therefore, implementing Zero Trust principles within the data plane can help to improve the security and resilience of the network.

One of the key principles of Zero Trust is to assume breach and minimize the blast radius and segment access. This means that the network should be divided into smaller and isolated segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot easily move laterally to other segments and access more resources or data. This principle is also known as threat scope reduction, as it reduces the scope and impact of a potential threat.

The other options are not as relevant for the data plane as threat scope reduction. Secured zones are a concept related to the control plane, which is the part of the network that makes routing and switching decisions. Subject role is a concept related to the identity plane, which is the part of the network that authenticates and authorizes users and devices. Adaptive identity is a concept related to the policy plane, which is the part of the network that defines and enforces the security policies and rules.

References = <https://bing.com/search?q=Zero+Trust+data+plane>

<https://learn.microsoft.com/en-us/security/zero-trust/deploy/data>

Questions # 91:

Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

Options:

A.

VM escape

B.

SQL injection

C.

Buffer overflow

D.

Race condition



CertsMania

Answer

C

Explanation

A buffer overflow is a vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. A register is a small storage area in the CPU that holds temporary data or instructions. An attacker can exploit a buffer overflow to overwrite a register with a malicious address that points to a shellcode, which is a piece of code that gives the attacker control over the system. By doing so, the attacker can bypass the normal execution flow of the application and execute arbitrary commands.

[References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Threats, Attacks, and Vulnerabilities, Section 2.3: Application Attacks, Page 76 1; Buffer Overflows - CompTIA Security+ SY0-701 - 2.3 2, , , , , , , ,]

Questions # 92:

Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

Options:

A.

Impact analysis

B.

Scheduled downtime

C.

Backout plan



CertsMania

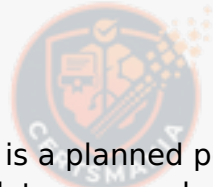
D.

Change management boards

Answer

B

Explanation



CertsMania

Scheduled downtime is a planned period of time when a system or service is unavailable for maintenance, updates, upgrades, or other changes. Scheduled downtime gives administrators a set period to perform changes to an operational system without disrupting the normal business operations or affecting the availability of the system or service. Scheduled downtime also allows administrators to inform the users and stakeholders about the expected duration and impact of the changes. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 12: Security Operations and Administration, page 579 1

Questions # 93:

Which of the following is a social engineering attack in which a bad actor impersonates a web URL?

Options:

A.

Pretexting

B.

Misinformation

C.

Typosquatting

D.

Watering-hole



CertsMania

Answer

C

Explanation

Typosquatting is a social engineering and cybersquatting technique in which attackers register domain names similar to legitimate ones, hoping users will make a typographical error and visit their malicious website instead.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 2.2: "Typosquatting involves registering misspelled versions of legitimate domain names to trick users.", Exam Objectives 2.2: "Given a scenario, analyze potential indicators associated with application attacks.", , , , , ,]

Questions # 94:

Which of the following cryptographic solutions protects data at rest?

Options:

- A.
Digital signatures
- B.
Full disk encryption
- C.
Private key
- D.
Steganography



CertsMania

Answer

B

Questions # 95:

A service provider wants a cost-effective way to rapidly expand from providing internet links to

managing them. Which of the following methods will allow the service provider to best scale its services while maintaining performance consistency?

Options:

- A.
Escalation support
- B.
Increased workforce
- C.
Baseline enforcement
- D.
Technical debt



CertsMania

Answer

C

Explanation

Baseline enforcement involves establishing standard configurations and operational baselines that allow a service provider to scale services efficiently while ensuring consistent performance and security. By enforcing baselines, automation can be applied, reducing manual intervention and variability, which supports rapid, cost-effective expansion.

Increasing workforce (B) adds operational cost and may introduce inconsistency. Escalation support (A) is reactive and does not inherently support scaling. Technical debt (D) refers to accumulated suboptimal design or quick fixes that hamper future scalability and is a negative factor.

Baseline enforcement is recognized as a best practice in the Security Program Management domain for scaling services reliably [6:Chapter 16†CompTIA Security+ Study Guide].

Questions # 96:

A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the

future?

Options:

A.

Tuning

B.

Aggregating

C.

Quarantining

D.

Archiving



CertsMania

Answer

A

Explanation

Tuning is the activity of adjusting the configuration or parameters of a security tool or system to optimize its performance and reduce false positives or false negatives. Tuning can help to filter out the normal or benign activity that is detected by the security tool or system, and focus on the malicious or anomalous activity that requires further investigation or response. Tuning can also help to improve the efficiency and effectiveness of the security operations center by reducing the workload and alert fatigue of the analysts. Tuning is different from aggregating, which is the activity of collecting and combining data from multiple sources or sensors to provide a comprehensive view of the security posture. Tuning is also different from quarantining, which is the activity of isolating a potentially infected or compromised device or system from the rest of the network to prevent further damage or spread. Tuning is also different from archiving, which is the activity of storing and preserving historical data or records for future reference or compliance. The act of ignoring detected activity in the future that is deemed normal by the security operations center is an example of tuning, as it involves modifying the settings or rules of the security tool or system to exclude the activity from the detection scope. Therefore, this is the best answer among the given options. References = Security Alerting and Monitoring Concepts and Tools - CompTIA Security+ SY0-701: 4.3, video at 7:00; CompTIA Security+ SY0-701 Certification Study Guide, page 191.

A systems administrator notices that one of the systems critical for processing customer transactions is running an end-of-life operating system. Which of the following techniques would increase enterprise security?

Options:

A.

Installing HIDS on the system

B.

Placing the system in an isolated VLAN

C.

Decommissioning the system

D.

Encrypting the system's hard drive

Answer

B

Explanation

To enhance security for a system running an end-of-life operating system, placing the system in an isolated VLAN is the most effective approach. By isolating the system from the rest of the network, you can limit its exposure to potential threats while maintaining its functionality. This segmentation helps protect the rest of the network from any vulnerabilities in the outdated system.

Installing HIDS (Host-based Intrusion Detection System) can help detect intrusions but won't mitigate the risks posed by an unsupported OS.

Decommissioning may not be feasible if the system is critical.

Encrypting the system's hard drive protects data at rest but doesn't address vulnerabilities from an outdated OS.

Questions # 98:

A network administrator wants to ensure that network traffic is highly secure while in transit. Which of the following actions best describes the actions the network administrator should take?

Options:

A.

Ensure that NAC is enforced on all network segments, and confirm that firewalls have updated policies to block unauthorized traffic.

B.

Ensure only TLS and other encrypted protocols are selected for use on the network, and only permit authorized traffic via secure protocols.

C.

Configure the perimeter IPS to block inbound HTTPS directory traversal traffic, and verify that signatures are updated on a daily basis.

D.

Ensure the EDR software monitors for unauthorized applications that could be used by threat actors, and configure alerts for the security team.

Answer

B

Questions # 99:

Which of the following is a prerequisite for a DLP solution?

Options:

A.

Data destruction

B.

Data sanitization

C.

Data classification

D.

Data masking

Answer

C

Explanation



CertsMania

Data classification is required before implementing a Data Loss Prevention (DLP) solution because DLP policies depend on identifying and categorizing sensitive data to monitor, block, or encrypt it accordingly.

Data destruction (A) and sanitization (B) remove data, and masking (D) obscures data but classification is foundational for DLP effectiveness.

Data classification is emphasized in Security Program Management and Data Protection topics [6:Chapter 16]†CompTIA Security+ Study Guide [6].

Questions # 100:

A security analyst has determined that a security breach would have a financial impact of \$15,000 and is expected to occur twice within a three-year period. Which of the following is the ALE for this risk?

Options:

A.

\$7,500

B.

\$10,000

C.

\$15,000

D.

\$30,000



CertsMania

Answer

B

Questions # 101:

Which of the following would most likely be used by attackers to perform credential harvesting?

Options:

A.

Social engineering

B.

Supply chain compromise

C.

Third-party software

D.

Rainbow table

Answer

A

Questions # 102:

An analyst identifies that multiple users have the same passwords, but the hashes appear to be completely different. Which of the following most likely explains this issue?

Options:

A.

Data masking

B.

Salting

C.

Key escrow

D.

Tokenization



CertsMania

Answer

B

Explanation

Salting involves adding a unique value (salt) to each password before hashing it. This means that even if two users have the same password, the added salts ensure their hash values are different. This protects against attacks that exploit identical hash values, such as rainbow table attacks.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 1.3, “Salting passwords ensures that identical passwords do not have identical hashes, even if the same hash algorithm is used.”, Exam Objectives 1.3: “Explain the importance of cryptographic concepts.”, , , , , ,]

Questions # 103:

While troubleshooting a firewall configuration, a technician determines that a “deny any” policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable.

Which of the following actions would prevent this issue?

Options:

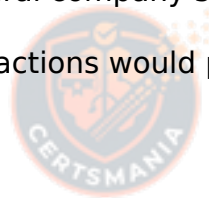
A.

Documenting the new policy in a change request and submitting the request to change management

B.

Testing the policy in a non-production environment before enabling the policy in the production network

C.



CertsMania

Disabling any intrusion prevention signatures on the 'deny any*' policy prior to enabling the new policy

D.

Including an 'allow any1 policy above the 'deny any* policy

Answer

B

Explanation



CertsMania

A firewall policy is a set of rules that defines what traffic is allowed or denied on a network. A firewall policy should be carefully designed and tested before being implemented, as a misconfigured policy can cause network disruptions or security breaches. A common best practice is to test the policy in a non-production environment, such as a lab or a simulation, before enabling the policy in the production network. This way, the technician can verify the functionality and performance of the policy, and identify and resolve any issues or conflicts, without affecting the live network. Testing the policy in a non-production environment would prevent the issue of the 'deny any' policy causing several company servers to become unreachable, as the technician would be able to detect and correct the problem before applying the policy to the production network.

Documenting the new policy in a change request and submitting the request to change management is a good practice, but it would not prevent the issue by itself. Change management is a process that ensures that any changes to the network are authorized, documented, and communicated, but it does not guarantee that the changes are error-free or functional. The technician still needs to test the policy before implementing it.

Disabling any intrusion prevention signatures on the 'deny any' policy prior to enabling the new policy would not prevent the issue, and it could reduce the security of the network. Intrusion prevention signatures are patterns that identify malicious or unwanted traffic, and allow the firewall to block or alert on such traffic. Disabling these signatures would make the firewall less effective in detecting and preventing attacks, and it would not affect the reachability of the company servers.

Including an 'allow any' policy above the 'deny any' policy would not prevent the issue, and it would render the 'deny any' policy useless. A firewall policy is processed from top to bottom, and the first matching rule is applied. An 'allow any' policy would match any traffic and allow it to pass through the firewall, regardless of the source, destination, or protocol. This would negate the purpose of the 'deny any' policy, which is to block any traffic that does not match any of the previous rules. Moreover, an 'allow any' policy would create a security risk, as it would allow any unauthorized or malicious traffic to enter or exit the network. References = CompTIA Security+ SY0-701 Certification Study Guide, page 204-205; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 2.1 - Network Security Devices, 8:00 - 10:00.

Questions # 104:

A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken first?

Options:

A.

Air gap the system.

B.

Move the system to a different network segment.

C.

Create a change control request.

D.

Apply the patch to the system.



CertsMania

Answer

C

Explanation

= A change control request is a document that describes the proposed change to a system, the reason for the change, the expected impact, the approval process, the testing plan, the implementation plan, the rollback plan, and the communication plan. A change control request is a best practice for applying any patch to a production system, especially a high-priority one, as it ensures that the change is authorized, documented, tested, and communicated. A change control request also minimizes the risk of unintended consequences, such as system downtime, data loss, or security breaches. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 235. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.1, page 13.

Questions # 105:

A security analyst learns that an attack vector, used as part of a recent incident, was a well-known IoT device exploit. The analyst needs to review logs to identify the time of the initial

exploit. Which of the following logs should the analyst review first?

Options:

A.

Endpoint

B.

Application

C.

Firewall

D.

NAC



CertsMania

Answer

A

Explanation

Detailed Explanation:Firewall logs provide details of all network traffic, including connections to and from IoT devices. They are typically the first source of evidence for identifying the time of an exploit. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Log Analysis for Incident Response".

Questions # 106:



CertsMania

Which of the following is a compensating control for providing user access to a high-risk website?

Options:

A.

Enabling threat prevention features on the firewall

B.

Configuring a SIEM tool to capture all web traffic

C.

Setting firewall rules to allow traffic from any port to that destination

D.

Blocking that website on the endpoint protection software

Answer

A



CertsMania

Questions # 107:

An employee from the accounting department logs in to the website used for processing the company's payments. After logging in, a new desktop application automatically downloads on the employee's computer and causes the computer to restart. Which of the following attacks has occurred?

Options:

A.

XSS

B.

Watering hole

C.

Typosquatting

D.

Buffer overflow



CertsMania

Answer

B

Explanation

A watering hole attack occurs when attackers compromise a website that is frequently visited by targeted users—in this case, the payment processing site used by employees.

The compromised site then delivers malicious payloads to visitors, such as downloading malicious applications without user consent.

XSS (Cross-Site Scripting) attacks inject malicious scripts into web pages but typically do not cause automatic application downloads leading to restarts. Typosquatting (C) involves malicious websites mimicking legitimate ones via misspelled URLs. Buffer overflow (D) is an attack targeting software memory but doesn't typically involve website compromise and automatic downloads.

This attack type is detailed in the Threats, Vulnerabilities, and Mitigations domain of SY0-701 [6]: Chapter 2†CompTIA Security+ Study Guide [6].

Questions # 108:

Which of the following mitigation techniques would a security analyst most likely use to avoid bloatware on devices?

Options:

A.

Disabled ports/protocols

B.

Application allow list

C.

Default password changes

D.

Access control permissions

Answer

B

Explanation

Application allow listing is the most effective technique to prevent bloatware, unauthorized software, or unnecessary applications from running on devices. Allow lists work by permitting only pre-approved, trusted applications to execute, blocking everything else by default. This is a recommended best practice in Security+ SY0-701 for reducing attack surface, preventing malware, and maintaining lean, hardened system

images.

Bloatware often comes pre-installed on devices or is unintentionally installed by users. An allow list ensures only authorized applications required for business functions can run, thereby eliminating bloatware risks.

Disabling ports/protocols (A) hardens network access but does not prevent software installation. Default password changes (C) improve authentication security but are unrelated to software control. Access control permissions (D) restrict who can access what but do not prevent installation of unnecessary apps.

Thus, the correct answer is B: Application allow list.

Questions # 109:

A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

Options:

A.

Accept

B.

Transfer

C.

Mitigate

D.

Avoid

Answer

B

Explanation

Cyber insurance is a type of insurance that covers the financial losses and liabilities that result from cyberattacks, such as data breaches, ransomware, denial-of-service, phishing, or malware. Cyber insurance can help a company recover from the costs of restoring data, repairing systems, paying ransoms, compensating customers, or facing legal actions.

Cyber insurance is one of the possible strategies that a company can use to address the items listed on the risk register. A risk register is a document that records the identified risks, their probability, impact, and mitigation strategies for a project or an organization. The four common risk mitigation strategies are:

Accept: The company acknowledges the risk and decides to accept the consequences without taking any action to reduce or eliminate the risk. This strategy is usually chosen when the risk is low or the cost of mitigation is too high.

Transfer: The company transfers the risk to a third party, such as an insurance company, a vendor, or a partner. This strategy is usually chosen when the risk is high or the company lacks the resources or expertise to handle the risk.

Mitigate: The company implements controls or measures to reduce the likelihood or impact of the risk. This strategy is usually chosen when the risk is moderate or the cost of mitigation is reasonable.

Avoid: The company eliminates the risk by changing the scope, plan, or design of the project or the organization. This strategy is usually chosen when the risk is unacceptable or the cost of mitigation is too high.

By purchasing cyber insurance, the company is transferring the risk to the insurance company, which will cover the financial losses and liabilities in case of a cyberattack. Therefore, the correct answer is B. Transfer. References = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 377. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.1: Risk Management, video: Risk Mitigation Strategies (5:37).

Questions # 110:

After reviewing the following vulnerability scanning report:

Server:192.168.14.6

Service: Telnet

Port: 23 Protocol: TCP

Status: Open Severity: High

Vulnerability: Use of an insecure network protocol

A security analyst performs the following test:

```
nmap -p 23 192.168.14.6 --script telnet-encryption
```

```
PORT STATE SERVICE REASON
```



CertsMania

23/tcp open telnet syn-ack

| telnet encryption:

|_ Telnet server supports encryption

Which of the following would the security analyst conclude for this reported vulnerability?

Options:

A.

It is a false positive.

B.

A rescan is required.

C.

It is considered noise.

D.

Compensating controls exist.



CertsMania

Answer

A

Explanation

A false positive is a result that indicates a vulnerability or a problem when there is none. In this case, the vulnerability scanning report shows that the telnet service on port 23 is open and uses an insecure network protocol. However, the security analyst performs a test using nmap and a script that checks for telnet encryption support. The result shows that the telnet server supports encryption, which means that the data transmitted between the client and the server can be protected from eavesdropping. Therefore, the reported vulnerability is a false positive and does not reflect the actual security posture of the server. The security analyst should verify the encryption settings of the telnet server and client and ensure that they are configured properly³. References: 3: Telnet Protocol - Can You Encrypt Telnet?

Questions # 111:

A security engineer is installing an IPS to block signature-based attacks in the environment.

Which of the following modes will best accomplish this task?

Options:

- A.
Monitor
- B.
Sensor
- C.
Audit
- D.
Active



CertsMania

Answer

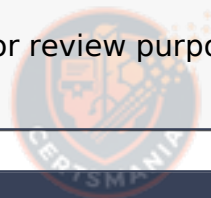
D

Explanation

To block signature-based attacks, the Intrusion Prevention System (IPS) must be in active mode. In this mode, the IPS can actively monitor and block malicious traffic in real time based on predefined signatures. This is the best mode to prevent known attack types from reaching the internal network.

Monitor mode and sensor mode are typically passive, meaning they only observe and log traffic without actively blocking it.

Audit mode is used for review purposes and does not actively block traffic.



CertsMania

Questions # 112:

A company's accounting department receives an urgent payment message from the company's bank domain with instructions to wire transfer funds. The sender requests that the transfer be completed as soon as possible. Which of the following attacks is described?

Options:

- A.

Business email compromise

B.

Vishing

C.

Spear phishing

D.

Impersonation



CertsMania

Answer

A

Explanation

This is a classic example of Business Email Compromise (BEC), where attackers spoof or compromise trusted email accounts to trick employees into performing unauthorized financial transactions.

Vishing (B) is voice phishing, spear phishing (C) targets individuals with customized messages, and impersonation (D) is a general term for identity deception but BEC specifically describes financial fraud via email.

BEC is a major threat covered in the Threats domain of SY0-701 6:Chapter 2†CompTIA Security+ Study Guide

Questions # 113:

In a rush to meet an end-of-year business goal, the IT department was told to implement a new business application. The security engineer reviews the attributes of the application and decides the time needed to perform due diligence is insufficient from a cybersecurity perspective. Which of the following best describes the security engineer's response?

Options:

A.

Risk tolerance

B.

Risk acceptance

C.

Risk importance

D.

Risk appetite



CertsMania

Answer

D

Explanation

Risk appetite refers to the level of risk that an organization is willing to accept in order to achieve its objectives. In this scenario, the security engineer is concerned that the timeframe for implementing a new application does not allow for sufficient cybersecurity due diligence. This reflects a situation where the organization's risk appetite might be too high if it proceeds without the necessary security checks.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of risk management and understanding organizational risk appetite.

Questions # 114:

Which of the following prevents unauthorized modifications to internal processes, assets, and security controls?

Options:

A.

Change management

B.

Playbooks

C.

Incident response

D.



CertsMania

Acceptable use policy

Answer

A

Explanation

Change management is the formal process designed to control, document, approve, and track modifications to systems, internal processes, assets, and security controls. This control mechanism helps prevent unauthorized or unintended changes that could introduce vulnerabilities or disrupt operations.

Playbooks are documented procedures for responding to incidents, incident response manages security incidents, and acceptable use policies define acceptable user behavior but do not directly control changes.

By enforcing proper change management, organizations maintain the integrity and security of their infrastructure, which is a critical topic covered in the Security Program Management and Oversight domain of SY0-701. Chapter 16 of CompTIA Security+ Study Guide.

Questions # 115:

An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?

Options:

A.

Smishing

B.

Disinformation

C.

Impersonating

D.

Whaling



CertsMania

Answer

D

Explanation

Whaling is a type of phishing attack that targets high-profile individuals, such as executives, celebrities, or politicians. The attacker impersonates someone with authority or influence and tries to trick the victim into performing an action, such as transferring money, revealing sensitive information, or clicking on a malicious link. Whaling is also called CEO fraud or business email compromise2.

[References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 97., , , , , , , ,]

Questions # 116:

After a series of account compromises and credential misuse, a company hires a security manager to develop a security program. Which of the following steps should the security manager take first to increase security awareness?

Options:

A.

Evaluate tools that identify risky behavior and distribute reports on the findings.

B.

Send quarterly newsletters that explain the importance of password management.

C.

Develop phishing campaigns and notify the management team of any successes.

D.

Update policies and handbooks to ensure all employees are informed of the new procedures.

Answer

D

Questions # 117:

An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?

Options:

A.

Hardening

B.

Employee monitoring

C.

Configuration enforcement

D.

Least privilege



CertsMania

Answer

D

Explanation

The principle of least privilege is a security concept that limits access to resources to the minimum level needed for a user, a program, or a device to perform a legitimate function. It is a cybersecurity best practice that protects high-value data and assets from compromise or insider threat. Least privilege can be applied to different abstraction layers of a computing environment, such as processes, systems, or connected devices. However, it is rarely implemented in practice.

In this scenario, the IT manager is setting up the principle of least privilege by restricting access to the administrator console of the help desk software to only two authorized users: the IT manager and the help desk lead. This way, the IT manager can prevent unauthorized or accidental changes to the software configuration, data, or functionality by other help desk staff. The other help desk staff will only have access to the normal user interface of the software, which is sufficient for them to perform their job functions.

The other options are not correct. Hardening is the process of securing a system by reducing its surface of vulnerability, such as by removing unnecessary software, changing default passwords, or disabling unnecessary services. Employee monitoring is the surveillance of workers' activity, such as by tracking web browsing, application use, keystrokes, or screenshots. Configuration enforcement is the process of ensuring that a system adheres to a predefined set of security settings, such as by applying a patch, a

policy, or a template.

References =

https://en.wikipedia.org/wiki/Principle_of_least_privilege

https://en.wikipedia.org/wiki/Principle_of_least_privilege

Questions # 118:

A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of users. Which of the following would be a good use case for this task?creating a script

Options:

A.

Off-the-shelf software

B.

Orchestration

C.

Baseline

D.

Policy enforcement

Answer

B

Explanation

In the context of the CompTIA Security+ SY0-701 exam, orchestration is the most appropriate answer because it directly aligns with the automation of repetitive, operational security tasks. Orchestration refers to the coordinated execution of automated processes to streamline workflows, reduce administrative burden, and ensure consistent outcomes. Creating a script to automate user account creation for a large number of users is a textbook example of orchestration in action.

The Security+ SY0-701 study guide emphasizes that automation and orchestration are

essential components of modern security operations. They are used to minimize human error, improve efficiency, and enforce consistency across environments. Manual account creation is error-prone, especially at scale, and can lead to misconfigured permissions, inconsistent group memberships, or skipped security steps. Orchestration ensures that predefined steps—such as creating user accounts, assigning roles, applying access controls, enforcing password policies, and logging actions—are executed reliably every time.

The other options do not fit the scenario. Off-the-shelf software refers to prebuilt commercial solutions rather than a custom script. A baseline defines a standard configuration state but does not automate actions. Policy enforcement ensures compliance with rules but does not perform the operational task itself. The key distinction is that orchestration focuses on execution and coordination of tasks, not governance or standards.

From a Security+ operational standpoint, orchestration supports secure identity and access management by ensuring accounts are provisioned consistently and in alignment with organizational policies. It also improves auditability and accountability by enabling predictable, repeatable processes. Therefore, orchestration is the correct and most secure solution for automating large-scale account creation.

Questions # 119:

Which of the following would best allow a company to prevent access to systems from the Internet?

Options:

A.

Containerization

B.

Virtualization

C.

SD-WAN

D.

Air-gapped



CertsMania

Answer

D

Explanation

An air-gapped system is physically isolated from unsecured networks (like the public Internet), ensuring that there is no direct or indirect network connection. This is the most effective way to prevent Internet-based access to sensitive systems.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 3.2: "Air-gapped systems are isolated from external networks and prevent Internet access.", Exam Objectives 3.2: "Summarize security implications of embedded and specialized systems.", , , , ,]

Questions # 120:

During a routine audit, an analyst discovers that a department at a high school uses a simulation program that was not properly vetted before deployment.

Which of the following threats is this an example of?

Options:

A.

Espionage

B.

Data exfiltration

C.

Shadow IT

D.

Zero-day



CertsMania

Answer

C

Questions # 121:

A company is aware of a given security risk related to a specific market segment. The business chooses not to accept responsibility and target their services to a different market segment. Which of the following describes this risk management strategy?

Options:

A.

Exemption

B.

Exception

C.

Avoid

D.

Transfer



CertsMania

Answer

C

Explanation

Detailed Explanation: Avoidance involves choosing not to engage in activities or markets where certain risks are present. This is a proactive approach to risk management.

Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Risk Management Strategies".



CertsMania

Questions # 122:

Which of the following can be used to mitigate attacks from high-risk regions?

Options:

A.

Obfuscation

B.

Data sovereignty

C.

IP geolocation

D.

Encryption



CertsMania

Answer

C

Questions # 123:

A company evaluates several options that would allow employees to have remote access to the network. The security team wants to ensure the solution includes AAA to comply with internal security policies. Which of the following should the security team recommend?

Options:

A.

IPSec with RADIUS

B.

RDP connection with LDAPS

C.

Web proxy for all remote traffic

D.

Jump server with 802.1X



CertsMania

Answer

A

Questions # 124:

A systems administrator is concerned users are accessing emails through a duplicate site that is not run by the company. Which of the following is used in this scenario?

Options:

- A.
Impersonation
- B.
Replication
- C.
Phishing
- D.
Smishing



CertsMania

Answer

A

Questions # 125:

A new corporate policy requires all staff to use multifactor authentication to access company resources. Which of the following can be utilized to set up this form of identity and access management? (Select two)

Options:

- A.
Authentication tokens
- B.
Least privilege
- C.
Biometrics



CertsMania

D.

LDAP

E.

Password vaulting

F.

SAML



CertsMania

Answer

A, C

Explanation

Multifactor authentication (MFA) requires users to provide two or more of the following categories:

Something you know (password/PIN)

Something you have (token/smart card)

Something you are (biometrics)

Authentication tokens (A) qualify as something you have, such as hardware tokens, OTP apps, or smart cards.

Biometrics (C) qualify as something you are, such as fingerprint scans, facial recognition, or iris scans. Using these two together easily establishes MFA.

Least privilege (B) is an authorization principle, not an MFA factor. LDAP (D) is a directory service protocol, not an MFA mechanism. Password vaulting (E) assists with credential storage but does not implement MFA. SAML (F) is a federation protocol used for Single Sign-On (SSO), not inherently MFA.

Thus, the correct MFA components are A: Authentication tokens and C: Biometrics.

Questions # 126:

A Chief Information Security Officer (CISO) has developed information security policies that relate to the software development methodology. Which of the following would the CISO most likely include in the organization's documentation?

Options:

A.

Peer review requirements

B.

Multifactor authentication

C.

Branch protection tests

D.

Secrets management configurations



CertsMania

Answer

A

Questions # 127:

A company is experiencing issues with employees leaving the company for a competitor and taking customer contact information with them. Which of the following tools will help prevent this from reoccurring?

Options:

A.

FIM

B.

NAC

C.

IDS

D.

UBA



CertsMania

Answer

D

Explanation

User Behavior Analytics (UBA) monitors user activities and detects anomalous behavior such as unauthorized data access or exfiltration, including when employees attempt to copy sensitive customer contact information before leaving. UBA can alert security teams to insider threats proactively.

File Integrity Monitoring (FIM) (A) detects unauthorized changes to files but is less effective against data exfiltration by insiders. Network Access Control (NAC) (B) controls device access to the network, and Intrusion Detection Systems (IDS) (C) detect suspicious network activity but do not specifically analyze user behaviors.

UBA is a critical tool for insider threat detection covered in Security Operations [6]:Chapter 14†CompTIA Security+ Study Guide [1].

Questions # 128:

Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

Options:

A.

SIEM

B.

DLP

C.

IDS

D.

SNMP

Answer

A

Explanation

SIEM stands for Security Information and Event Management. It is a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system. SIEM can analyze the collected data, correlate events, generate alerts, and provide reports and dashboards. SIEM can also integrate with other security tools and support compliance requirements. SIEM helps organizations to detect and respond to cyber threats, improve security posture, and reduce operational costs. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Monitoring and Auditing, page 393. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 10: Monitoring and Auditing, page 397.

Questions # 129:

Which of the following documents details how to accomplish a technical security task?

Options:

A.

Standard

B.

Policy

C.

Guideline

D.

Procedure



CertsMania

Answer

D

Explanation

A procedure provides step-by-step instructions on how to complete a specific security task, ensuring consistency and accuracy. Unlike policies, which define high-level security expectations, procedures are detailed and operational. For example, a password reset procedure would outline the exact steps IT support must follow when assisting users.

Policy: Defines security objectives and rules (e.g., "All passwords must be complex").

Standard: Specifies required technologies or configurations.

Guideline: Provides recommendations but is not mandatory.

Procedure: Gives exact instructions to perform tasks.

[Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain., , , , , ,]

Questions # 130:

Which of the following steps in the risk management process involves establishing the scope and potential risks involved with a project?

Options:

A.

Risk mitigation

B.

Risk identification

C.

Risk treatment

D.

Risk monitoring and review

Answer

B

Explanation

Risk identification is the first step in the risk management process, where potential threats and vulnerabilities are analyzed to understand their impact on an organization. This includes identifying assets, evaluating threats, and assessing potential vulnerabilities.

Risk mitigation: Reducing risk by implementing controls.

Risk treatment: Determining how to handle identified risks.

Risk monitoring and review: Ongoing evaluation of risk controls.

[Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain., , , , , ,]

Questions # 131:

Which of the following is the most relevant reason a DPO would develop a data inventory?

Options:

- A.
To manage data storage requirements better
- B.
To determine the impact in the event of a breach
- C.
To extend the length of time data can be retained
- D.
To automate the reduction of duplicated data

Answer

B

Questions # 132:

Which of the following allows a systems administrator to tune permissions for a file?

Options:

- A.
Patching
- B.
Access control list

C.

Configuration enforcement

D.

Least privilege

Answer

B

Explanation

Detailed Explanation: Access control lists (ACLs) allow administrators to fine-tune file permissions by specifying which users or groups have access to a file and defining the level of access. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Access Control Mechanisms".

Questions # 133:

Which of the following is the greatest advantage that network segmentation provides?

Options:

A.

End-to-end encryption

B.

Decreased resource utilization

C.

Enhanced endpoint protection

D.

Configuration enforcement

E.

Security zones

Answer

E

Explanation

Comprehensive and Detailed Explanation From Exact Extract:

The greatest advantage of network segmentation is the creation of security zones, which isolate systems into separate logical or physical network sections. According to CompTIA Security+ SY0-701, segmentation is a foundational security architecture practice used to reduce the attack surface, restrict lateral movement, enforce least privilege, and contain breaches. By dividing the network into zones—such as DMZ, internal, restricted, and guest—administrators can apply tailored access controls, firewall rules, IDS/IPS placement, and monitoring boundaries.

Segmentation provides defense-in-depth by preventing attackers from reaching critical systems even if they compromise a less-secure device. It also limits broadcast domains and improves traffic visibility. End-to-end encryption (A) protects confidentiality but is unrelated to segmentation. Decreased resource utilization (B) is not a primary benefit. Enhanced endpoint protection (C) applies to host controls, not network topology. Configuration enforcement (D) is a benefit of centralized management, not segmentation.

Therefore, the correct answer is Security zones, the core outcome and highest-value advantage of segmentation.

Questions # 134:

Which solution is most likely used in the financial industry to mask sensitive data?

Options:

A.

Tokenization

B.

Hashing

C.

Salting

D.

Steganography



CertsMania

Answer

A

Explanation

Tokenization replaces sensitive financial data—such as credit card numbers, account numbers, or customer identifiers—with harmless tokens that retain usability but reveal nothing if leaked. This is widely used in the financial industry, particularly in PCI-DSS-regulated systems.

Hashing (B) is one-way and not reversible, making it unsuitable for financial transactions that need original data retrieved. Salting (C) is used to protect hashed passwords, not to mask financial data. Steganography (D) hides data inside media files but is not used for payment processing.

Security+ SY0-701 identifies tokenization as the preferred method for protecting structured sensitive data while maintaining operational functionality.

Thus, the correct answer is A: Tokenization.

Questions # 135:

A company suffered a critical incident where 30GB of data was exfiltrated from the corporate network. Which of the following actions is the most efficient way to identify where the system data was exfiltrated from and where it was sent?

Options:

A.

Analyze firewall and network logs for large amounts of outbound traffic to external IP addresses or domains.

B.

Analyze IPS and IDS logs to find the IP addresses used by the attacker for reconnaissance scans.

C.

Analyze endpoint and application logs to see whether file-sharing programs were running.

D.

Analyze external vulnerability scans to identify exploitable systems.

Answer

A

Explanation

To efficiently identify where data was exfiltrated from and where it was sent, the best action is to analyze firewall and network logs for unusually large outbound data transfers. Security+ SY0-701 emphasizes that network-level telemetry provides the most direct evidence of data exfiltration, including source IPs, destination IPs or domains, ports, protocols, timestamps, and data volume.

Firewall and flow logs can quickly reveal which internal systems transmitted large quantities of data externally and identify the attacker's destination infrastructure. This approach is efficient because it focuses directly on the movement of data rather than preliminary or secondary indicators.

IPS/IDS logs (B) are more useful for detecting reconnaissance or intrusion attempts, not confirming data theft paths. Endpoint and application logs (C) may help identify tools used but are less efficient for mapping data movement. External vulnerability scans (D) identify weaknesses, not exfiltration activity.

Therefore, the most efficient action is A: Analyze firewall and network logs for large outbound traffic.

Questions # 136:

A company's Chief Information Security Officer (CISO) wants to enhance the capabilities of the incident response team. The CISO directs the incident response team to deploy a tool that rapidly analyzes host and network data from potentially compromised systems and forwards the data for further review. Which of the following tools should the incident response team deploy?

Options:

- A.
NAC
- B.
IPS
- C.

SIEM

D.

EDR

Answer

D

Explanation



CertsMania

Comprehensive and Detailed In-Depth Explanation:

An Endpoint Detection and Response (EDR) solution is designed to monitor, detect, and respond to security incidents on endpoints (such as workstations and servers). It collects and analyzes data, detecting suspicious activity and forwarding relevant information for further investigation.

Network Access Control (NAC) (A) enforces network access policies but does not analyze security threats on hosts.

Intrusion Prevention Systems (IPS) (B) detect and block network threats but do not provide deep endpoint analytics.

Security Information and Event Management (SIEM) (C) aggregates logs and provides security analytics but lacks direct endpoint detection and response capabilities.

EDR is the best choice for analyzing and responding to endpoint security incidents.

Questions # 137:

An organization has too many variations of a single operating system and needs to standardize the arrangement prior to pushing the system image to users. Which of the following should the organization implement first?

Options:

A.

Standard naming convention

B.

Mashing

C.

Network diagrams

D.

Baseline configuration

Answer

D

Explanation

Baseline configuration is the process of standardizing the configuration settings for a system or network. In this scenario, the organization needs to standardize the operating system configurations before deploying them across the network. Establishing a baseline configuration ensures that all systems adhere to the organization's security policies and operational requirements.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of system hardening and configuration management.

Questions # 138:

Which of the following are the best methods for hardening end user devices? (Select two)

Options:

A.

Full disk encryption

B.

Group-level permissions

C.

Account lockout

D.

Endpoint protection

E.

Proxy server

F.

Segmentation

Answer

A, D

Explanation



CertsMania

The best methods for hardening end user devices are Full Disk Encryption (FDE) and Endpoint Protection. FDE (A) protects data at rest on laptops and workstations, ensuring that data remains unreadable if devices are lost or stolen—an explicit best practice in Security+ SY0-701.

Endpoint protection (D), including EDR/anti-malware, hardens devices by preventing, detecting, and responding to malicious activity at the host level. Together, these controls provide strong baseline protection for confidentiality and threat prevention.

Group-level permissions (B) and account lockout (C) are important access controls but do not comprehensively harden devices against malware and data exposure. Proxy servers (E) and segmentation (F) are network controls rather than endpoint hardening measures.

Therefore, the correct selections are A: Full disk encryption and D: Endpoint protection.

Explanation (Security+ SY0-701 aligned):

Deception technologies—such as honeypots, honeynets, honeyfiles, and honeytokens—are designed to intentionally lure attackers into controlled, monitored environments. Their primary purpose is not to block attacks outright or replace preventive controls, but to observe attacker behavior, techniques, and tools in a safe way. This allows organizations to collect high-value threat intelligence without exposing real production systems or sensitive data.

In the Security+ SY0-701 objectives (General Security Concepts), deception and disruption technologies are highlighted as tools that increase attacker cost and uncertainty while improving defender visibility. When an attacker interacts with a honeypot or accesses a honeyfile, it generates a strong indicator of malicious intent because legitimate users should never touch these resources. This makes deception technologies extremely valuable for early detection and analysis of attacks.

Why the other options are incorrect:

A. Preventing malware installation is the role of endpoint protection platforms (EPP/EDR), not deception technologies.

B. Blocking all external traffic before it reaches critical systems describes perimeter defenses like firewalls or gateways, not deception.

D. Detecting insider threats by monitoring privileged accounts is handled by IAM controls, logging, and UEBA, not deception systems.

In short, deception technologies are proactive detection and intelligence-gathering tools. They don't stop attackers at the gate; instead, they trick attackers into revealing themselves and their methods, giving defenders insight that strengthens the overall security strategy.

Explanation (Security+ SY0-701 aligned):

To ensure an organization can review the controls and performance of a service provider or vendor, it should include a right-to-audit clause in its contract. A right-to-audit clause explicitly grants the customer the legal authority to inspect, assess, or audit the vendor's security controls, processes, and compliance posture. This is a key concept under Security Program Management and Oversight, particularly within third-party risk management.

In the SY0-701 objectives, third-party risk management emphasizes the importance of contractual controls that allow organizations to verify that vendors are meeting security, privacy, and compliance obligations. A right-to-audit clause enables activities such as reviewing policies, examining control effectiveness, validating compliance with standards (for example, SOC reports), and confirming that agreed-upon safeguards are actually in place. Without this clause, the organization may have no formal mechanism to independently verify vendor claims.

Why the other options are incorrect:

A. Service-level agreement (SLA): SLAs define performance metrics like uptime, response time, and availability. They do not usually grant audit authority over security controls.

B. Memorandum of agreement (MOA): An MOA outlines general responsibilities and cooperation between parties but typically lacks enforceable audit rights.

D. Supply chain analysis: This is a risk assessment activity, not a contractual mechanism that provides audit access.

From a Security+ perspective, the right-to-audit clause is the most effective and direct way to ensure ongoing visibility and assurance over vendor security controls and performance.

Questions # 139:

Which of the following should an organization focus on the most when making decisions about vulnerability prioritization?

Options:

A.

Exposure factor

B.

CVSS

C.

CVE

D.

Industry impact



CertsMania

Answer

B

Explanation

Detailed Explanation: The Common Vulnerability Scoring System (CVSS) is a standardized metric used to assess the severity of vulnerabilities, aiding organizations in prioritizing their response based on risk. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Vulnerabilities, Section: "Vulnerability Prioritization and Metrics".

Questions # 140:

An administrator learns that users are receiving large quantities of unsolicited messages. The administrator checks the content filter and sees hundreds of messages sent to multiple users. Which of the following best describes this kind of attack?

Options:

A.

Watering hole

B.

Typosquatting

C.

Business email compromise

D.



CertsMania

Answer

D

Explanation

The scenario describes a large number of unsolicited emails sent to multiple users. This is characteristic of phishing, which SY0-701 defines as mass-distributed fraudulent messages designed to trick recipients into clicking malicious links, downloading malware, or divulging sensitive information.

Phishing campaigns typically involve:

High volume

Non-targeted messaging

Use of spoofed addresses or fake content

Delivery through email systems

A watering-hole attack (A) compromises a legitimate website frequented by targets—not email. Typosquatting (B) relies on malicious websites with deceptive URLs. Business Email Compromise (C) involves highly targeted spear-phishing or impersonation attacks, not bulk email blasts.

Because this incident involves “hundreds of messages” delivered to “multiple users,” it clearly matches the characteristics of a phishing attack, not a sophisticated targeted attack type.

Phishing is the most common form of social engineering and is emphasized heavily in the Security+ exam due to its frequency and effectiveness.

Questions # 141:

Which of the following explains how to determine the global regulations that data is subject to regardless of the country where the data is stored?

Options:

A.

Geographic dispersion

B.

Data sovereignty

C.

Geographic restrictions

D.

Data segmentation



CertsMania

Answer

B

Questions # 142:

A network administrator deploys an FDE solution on all end user workstations. Which of the following data protection strategies does this describe?

Options:

A.

Masking

B.

Data in transit

C.

Obfuscation

D.

Data at rest

E.

Data sovereignty



CertsMania

Answer

D

Explanation

Full-disk encryption (FDE) protects the contents of storage media, which is a classic data-at-rest control. The Study Guide explains the “three situations” relevant to confidentiality—at rest, in transit, and in use—and then specifically ties disk encryption/FDE to protecting stored data: “Data at rest, or stored data, is that which resides in a permanent location awaiting access... Examples... hard drives...” It then describes FDE as an encryption method applied to disks: “Full-disk encryption (FDE) is a form of encryption where all the data on a hard drive is automatically encrypted, including the operating system and system files... In the case of loss or theft, FDE can prevent unauthorized access to all data on the hard drive.”

That is exactly the definition of protecting data at rest—it is intended to prevent disclosure if a laptop/workstation is lost, stolen, or the drive is removed. This is not masking (hiding parts of fields), not data in transit (network encryption like TLS/VPN), not obfuscation (making code hard to understand), and not data sovereignty (jurisdiction/location requirements). Therefore, deploying FDE on workstations is a data-at-rest protection strategy.

[References: Data-at-rest definition and confidentiality contexts ; FDE definition and purpose protecting disk-stored data . , ,]

Questions # 143:

An employee used a company's billing system to issue fraudulent checks. The administrator is looking for evidence of other occurrences of this activity. Which of the following should the administrator examine?

Options:

A.

Application logs

B.

Vulnerability scanner logs

C.

IDS/IPS logs

D.

Firewall logs



CertsMania

Answer

A

Questions # 144:

A database administrator is updating the company's SQL database, which stores credit card information for pending purchases. Which of the following is the best method to secure the data against a potential breach?

Options:

A.

Hashing

B.

Obfuscation

C.

Tokenization

D.

Masking

Answer

C

Questions # 145:

A security consultant is working with a client that wants to physically isolate its secure systems. Which of the following best describes this architecture?

Options:

A.

SDN

B.

Air gapped

C.

Containerized

D.

Highly available



CertsMania

Answer

B

Questions # 146:

A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider. Which of the following is a risk in the new system?

Options:

A.

Default credentials

B.

Non-segmented network

C.

Supply chain vendor

D.

Vulnerable software



CertsMania

Answer

C

Explanation

A supply chain vendor is a third-party entity that provides goods or services to an

organization, such as a SaaS provider. A supply chain vendor can pose a risk to the new system if the vendor has poor security practices, breaches, or compromises that could affect the confidentiality, integrity, or availability of the system or its data. The organization should perform due diligence and establish a service level agreement with the vendor to mitigate this risk. The other options are not specific to the scenario of using a SaaS provider, but rather general risks that could apply to any system.

Questions # 147:

Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?

Options:

- A.
Code scanning for vulnerabilities
- B.
Open-source component usage
- C.
Quality assurance testing
- D.
Peer review and approval

Answer

D

Explanation

Peer review and approval is a practice that involves having other developers or experts review the code before it is deployed or released. Peer review and approval can help detect and prevent malicious code, errors, bugs, vulnerabilities, and poor quality in the development process. Peer review and approval can also enforce coding standards, best practices, and compliance requirements. Peer review and approval can be done manually or with the help of tools, such as code analysis, code review, and code signing. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 543 2

Questions # 148:

The security operations center is researching an event concerning a suspicious IP address. A security analyst looks at the following event logs and discovers that a significant portion of the user accounts have experienced failed log-in attempts when authenticating from the same IP address:

>

Which of the following most likely describes attack that took place?

Options:

A.

Spraying

B.

Brute-force

C.

Dictionary

D.

Rainbow table

Answer

A

Explanation

Password spraying is a type of attack where an attacker tries a small number of commonly used passwords across a large number of accounts. The event logs showing failed login attempts for many user accounts from the same IP address are indicative of a password spraying attack, where the attacker is attempting to gain access by guessing common passwords.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management and common attack vectors like password spraying.

Questions # 149:

A security administrator observed the following in a web server log while investigating an incident:

>

Which of the following attacks did the security administrator most likely see?

Options:

- A.
Privilege escalation
- B.
Credential replay
- C.
Brute force
- D.
Directory traversal



CertsMania

Answer

D

Questions # 150:

Which of the following is the primary purpose of a service that tracks log-ins and time spent using the service?

Options:

- A.
Availability
- B.
Accounting
- C.



CertsMania

Authentication

D.

Authorization

Answer

B

Explanation



CertsMania

Accounting logs user activities such as log-ins and usage duration, which is part of the AAA framework (Authentication, Authorization, and Accounting).

=====

Questions # 151:

A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

Options:

A.

SSO

B.

LEAP

C.

MFA

D.

PEAP



CertsMania

Answer

A

Explanation

SSO stands for single sign-on, which is a method of authentication that allows users to access multiple applications or services with one set of credentials. SSO reduces the number of credentials employees need to maintain and simplifies the login process. SSO can also improve security by reducing the risk of password reuse, phishing, and credential theft. SSO can be implemented using various protocols, such as SAML, OAuth, OpenID Connect, and Kerberos, that enable the exchange of authentication information between different domains or systems. SSO is commonly used for accessing SaaS applications, such as Office 365, Google Workspace, Salesforce, and others, using domain credentials¹²³.

B. LEAP stands for Lightweight Extensible Authentication Protocol, which is a Cisco proprietary protocol that provides authentication for wireless networks. LEAP is not related to SaaS applications or domain credentials⁴.

C. MFA stands for multi-factor authentication, which is a method of authentication that requires users to provide two or more pieces of evidence to prove their identity. MFA can enhance security by adding an extra layer of protection beyond passwords, such as tokens, biometrics, or codes. MFA is not related to SaaS applications or domain credentials, but it can be used in conjunction with SSO.

D. PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that provides secure authentication for wireless networks. PEAP uses TLS to create an encrypted tunnel between the client and the server, and then uses another authentication method, such as MS-CHAPv2 or EAP-GTC, to verify the user's identity. PEAP is not related to SaaS applications or domain credentials.

References = 1: Security+ (SY0-701) Certification Study Guide | CompTIA IT Certifications 2: What is Single Sign-On (SSO)? - Definition from WhatIs.com 3: Single sign-on - Wikipedia 4: Lightweight Extensible Authentication Protocol - Wikipedia : What is Multi-Factor Authentication (MFA)? - Definition from WhatIs.com : Protected Extensible Authentication Protocol - Wikipedia

Questions # 152:

Which of the following data types best describes an AI tool developed by a company to automate the ticketing system under a specific contract?

Options:

A.

Classified

B.

Regulated information

C.

Open source

D.

Intellectual property



CertsMania

Answer

D

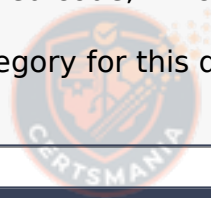
Explanation

An AI tool developed internally for automating a ticketing system represents intellectual property (IP). Security+ SY0-701 defines IP as proprietary creations developed by an organization, such as software, machine learning models, algorithms, and trade secrets. This type of data must be protected because it provides competitive advantage and is often contractually bound.

The scenario notes the tool is developed under a specific contract, meaning it is bound by ownership, licensing, and confidentiality agreements. Protecting IP is critical to prevent theft, unauthorized reuse, or compromise that could affect legal obligations or business value.

Classified (A) refers to government-protected national security information. Regulated information (B) includes data covered by laws such as HIPAA or PCI-DSS. Open source (C) refers to publicly shared code, which this AI tool is not.

Thus, the correct category for this data is D: Intellectual property.



CertsMania

Questions # 153:

Which of the following would be the best solution to deploy a low-cost standby site that includes hardware and internet access?

Options:

A.

Recovery site

B.

Cold site

C.

Hot site

D.

Warm site



CertsMania

Answer

B

Questions # 154:

An administrator is estimating the cost associated with an attack that could result in the replacement of a physical server. Which of the following processes is the administrator performing?

Options:

A.

Quantitative risk analysis

B.

Disaster recovery test

C.

Physical security controls review

D.

Threat modeling



CertsMania

Answer

A

Explanation

Quantitative risk analysis involves assigning numeric values to risk components, such as potential financial losses. Estimating the replacement cost of a physical server is part of calculating the potential impact and exposure during this process.

Disaster recovery tests (B) validate recovery procedures, physical security controls review (C) assesses physical protections, and threat modeling (D) identifies potential threats and attack vectors.

Quantitative analysis is a key part of risk management addressed in the SY0-701 Risk Management domain [6:Chapter 17†CompTIA Security+ Study Guide]

Questions # 155:

A company expects its provider to ensure servers and networks maintain 97% uptime. Which of the following would most likely list this expectation?

Options:

A.

BPA

B.

MOU

C.

NDA

D.

SLA

Answer

D

Explanation

An SLA (Service-Level Agreement) defines the expected performance, availability, uptime, response times, and responsibilities between a provider and a client. The requirement in the scenario—"97% uptime"—is a classic example of an SLA metric. Security+ SY0-701

emphasizes that SLAs outline measurable service expectations so the client can assess compliance and performance.

A BPA (A) outlines business partnership terms, not performance uptime. An MOU (B) documents mutual understanding but is not legally binding and does not include uptime metrics. An NDA (C) protects confidentiality, not availability or service guarantees.

Thus, the correct answer is D: SLA.

Questions # 156:

A company wants to track modifications to the code that is used to build new virtual servers. Which of the following will the company most likely deploy?

Options:

A.

Change management ticketing system

B.

Behavioral analyzer

C.

Collaboration platform

D.

Version control tool

Answer

D

Explanation

A version control tool, such as Git, is specifically designed to track changes in code, configuration scripts, IaC templates, and deployment files. In the context of creating new virtual servers—often built using Infrastructure as Code (IaC) or automated orchestration—version control allows teams to maintain historical records, compare changes, revert mistakes, ensure code integrity, and enable collaborative development.

Security+ SY0-701 emphasizes the use of version control in secure development practices to ensure traceability, accountability, and change visibility. It supports secure DevOps

workflows by ensuring that no unauthorized or insecure code modifications are introduced into production environments.

A change management ticketing system (A) documents approval requests but does not track code-level modifications. A behavioral analyzer (B) evaluates anomalous behavior, not code changes. A collaboration platform (C) enables communication but lacks code versioning capability.

Therefore, the most appropriate tool is D: Version control tool.

Questions # 157:

A company is in the process of cutting jobs to manage costs. The Chief Information Security Officer is concerned about the increased risk of an insider threat. Which of the following will most likely help the security awareness team address this potential threat?

Options:

A.

Immediately disable the accounts of staff who are likely to be terminated.

B.

Train supervisors to identify and manage disgruntled employees.

C.

Configure DLP to monitor staff who will be terminated.

D.

Raise awareness for business leaders on social engineering techniques.

Answer

B

Explanation

The correct answer is Train supervisors to identify and manage disgruntled employees because insider threat risk is strongly tied to human behavior, morale, and organizational change. In the Security+ SY0-701 framework, insider threats are not limited to technical weaknesses but are often driven by emotional, financial, or workplace stressors—such as layoffs, demotions, or job uncertainty. During workforce reductions, employees may experience resentment or fear, increasing the likelihood of malicious or negligent actions.

Security awareness programs are designed to address human-centric risks through education, observation, and early intervention. Training supervisors equips them to recognize warning signs of insider threat behavior, including sudden disengagement, policy violations, excessive access requests, or hostile workplace conduct. The SY0-701 study guide emphasizes that managers and supervisors are in the best position to observe behavioral changes and escalate concerns before they turn into security incidents.

Option A is incorrect because disabling accounts before termination can disrupt operations, violate HR procedures, and raise legal or ethical concerns. Option C, configuring DLP to monitor staff targeted for termination, may be inappropriate, legally risky, and reactive rather than preventive. Option D focuses on external threats like phishing and manipulation, not internal risks tied to layoffs.

By training supervisors, the organization strengthens administrative and operational controls that align with security governance and personnel risk management objectives in SY0-701. This proactive approach supports collaboration between HR, management, and security teams, ensuring insider threats are identified early and handled appropriately.

In summary, insider threat mitigation during layoffs is most effective when focused on people and processes. Training supervisors helps detect risk indicators early, supports employee well-being, and reduces the likelihood of intentional or accidental security incidents during periods of organizational stress.

Questions # 158:

During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?

Options:

A.

Analysis

B.

Lessons learned

C.

Detection

D.

Containment



CertsMania

Answer

A

Explanation

Analysis is the incident response activity that describes the process of understanding the source of an incident. Analysis involves collecting and examining evidence, identifying the root cause, determining the scope and impact, and assessing the threat actor's motives and capabilities. Analysis helps the incident response team to formulate an appropriate response strategy, as well as to prevent or mitigate future incidents. Analysis is usually performed after detection and before containment, eradication, recovery, and lessons learned. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 223. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.2, page 13.

Questions # 159:

Which of the following is an algorithm performed to verify that data has not been modified?

Options:

A.

Hash

B.

Code check

C.

Encryption

D.

Checksum



CertsMania

Answer

A

Explanation

A hash is an algorithm used to verify data integrity by generating a fixed-size string of

characters from input data. If even a single bit of the input data changes, the hash value will change, allowing users to detect any modification to the data. Hashing algorithms like SHA-256 and MD5 are commonly used to ensure data has not been altered.

[References:, CompTIA Security+ SY0-701 Course Content: Domain 6: Cryptography and PKI, which discusses the role of hashing in verifying data integrity., , , , ,]

Questions # 160:

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following best describes this step?

Options:

- A.
Capacity planning
- B.
Redundancy
- C.
Geographic dispersion
- D.
Tablet exercise

Answer

A

Explanation

Capacity planning is the process of determining the resources needed to meet the current and future demands of an organization. Capacity planning can help a company develop a business continuity strategy by estimating how many staff members would be required to sustain the business in the case of a disruption, such as a natural disaster, a cyberattack, or a pandemic. Capacity planning can also help a company optimize the use of its resources, reduce costs, and improve performance. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 184. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 4.1, page 14. Business Continuity - SY0-601 CompTIA Security+ : 4.1

Questions # 161:

Which of the following agreements defines response time, escalation points, and performance metrics?

Options:

A.

BPA

B.

MOA

C.

NDA

D.

SLA



CertsMania

Answer

D

Explanation

A Service Level Agreement (SLA) defines the expectations between service providers and customers, including response times, escalation procedures, and performance metrics. It ensures accountability and measurable service quality.

BPA (Blanket Purchase Agreement) relates to purchasing terms, MOA (Memorandum of Agreement) outlines responsibilities but is less specific on performance, NDA (Non-Disclosure Agreement) covers confidentiality.

SLAs are key in Security Program Management for managing vendor and internal service expectations [6:Chapter 16†CompTIA Security+ Study Guide].

Questions # 162:

A systems administrator is redesigning how devices will perform network authentication. The following requirements need to be met:

- An existing Internal certificate must be used.
- Wired and wireless networks must be supported
- Any unapproved device should be Isolated in a quarantine subnet
- Approved devices should be updated before accessing resources

Which of the following would best meet the requirements?

Options:

A.

802.1X

B.

EAP

C.

RADIUS

D.

WPA2

Answer

A

Explanation

802.1X is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. It supports the use of certificates for authentication, can quarantine unapproved devices, and ensures that only approved and updated devices can access network resources. This protocol best meets the requirements of securing both wired and wireless networks with internal certificates.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of network security and authentication protocols.

A few weeks after deploying additional email servers, a company begins to receive complaints that messages are going into recipients' spam folders. Which of the following needs to be updated?

Options:

A.

CNAME

B.

SMTP

C.

DLP

D.

SPF



CertsMania

Answer

D

Explanation

When new email servers are deployed, organizations must update their SPF (Sender Policy Framework) records to list the new servers as authorized senders. If the SPF DNS record does not include the new IP addresses, recipient mail systems cannot verify the legitimacy of the messages, causing them to be flagged as spam or rejected.

Security+ SY0-701 identifies SPF as a key email authentication mechanism responsible for preventing:

Email spoofing

Unauthorized sender impersonation

False spam detection

Domain reputation issues

CNAME (A) maps domain aliases but does not authenticate email. SMTP (B) is the mail protocol and does not influence spam classification. DLP (C) prevents data leakage, not spam filtering.

Updating the SPF record resolves legitimacy issues by informing receiving mail servers that the new email servers are trusted.

Thus, the correct answer is D: SPF.

Questions # 164:

A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?

Options:

A.

Deploying PowerShell scripts

B.

Pushing GPO update

C.

Enabling PAP

D.

Updating EDR profiles

Answer

B

Explanation

A group policy object (GPO) is a mechanism for applying configuration settings to computers and users in an Active Directory domain. By pushing a GPO update, the systems administrator can quickly and uniformly enforce the new password policy across all systems in the domain. Deploying PowerShell scripts, enabling PAP, and updating EDR profiles are not the most efficient or effective ways to change the password policy within an enterprise environment. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 115; Password Policy - Windows Security

Questions # 165:

Which of the following strategies should an organization use to efficiently manage and analyze multiple types of logs?

Options:

- A.
Deploy a SIEM solution
- B.
Create custom scripts to aggregate and analyze logs
- C.
Implement EDR technology
- D.
Install a unified threat management appliance



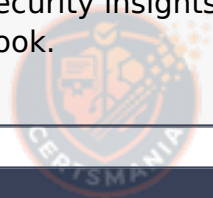
CertsMania

Answer

A

Explanation

Deploying a Security Information and Event Management (SIEM) solution allows for efficient log aggregation, correlation, and analysis across an organization's infrastructure, providing real-time security insights. References: Security+ SY0-701 Course Content, Security+ SY0-601 Book.



CertsMania

Questions # 166:

An administrator is Investigating an incident and discovers several users' computers were Infected with malware after viewing files mat were shared with them. The administrator discovers no degraded performance in the infected machines and an examination of the log files does not show excessive failed logins. Which of the following attacks Is most likely the cause of the malware?

Options:

A.

Malicious flash drive

B.

Remote access Trojan

C.

Brute-forced password

D.

Cryptojacking



CertsMania

Answer

D

Explanation

Cryptojacking is the likely cause in this scenario. It involves malware that hijacks the resources of infected computers to mine cryptocurrency, usually without the user's knowledge. This type of attack doesn't typically degrade performance significantly or result in obvious system failures, which matches the situation described, where the machines showed no signs of degraded performance or excessive failed logins.

References =

CompTIA Security+ SY0-701 Course Content: Cryptojacking is covered under types of malware attacks, highlighting its stealthy nature and impact on infected systems.



CertsMania

Questions # 167:

Employees located off-site must have access to company resources in order to complete their assigned tasks. These employees utilize a solution that allows remote access without interception concerns. Which of the following best describes this solution?

Options:

A.

Proxy server

B.

NGFW

C.

VPN

D.

Security zone



CertsMania

Answer

C

Explanation

A Virtual Private Network (VPN) is the best solution to allow remote employees secure access to company resources without interception concerns. A VPN establishes an encrypted tunnel over the internet, ensuring that data transferred between remote employees and the company is secure from eavesdropping.

Proxy server helps with web content filtering and anonymization but does not provide encrypted access.

NGFW (Next-Generation Firewall) enhances security but is not the primary tool for enabling remote access.

Security zone is a network segmentation technique but does not provide remote access capabilities.

Questions # 168:



CertsMania

Which of the following data protection strategies can be used to confirm file integrity?

Options:

A.

Masking

B.

Encryption

C.

Hashing

D.

Obfuscation

Answer

C

Explanation

Hashing (C) is a one-way cryptographic function that produces a fixed-length digest representing the original data. If the file changes—even by one bit—the hash will change, making it ideal for verifying data integrity.

While encryption protects confidentiality, and masking/obfuscation protect data visibility, only hashing ensures integrity.

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 1.2 - "Data protection methods: Hashing for integrity verification.", , , , , ,]

Questions # 169:

A visitor plugs a laptop into a network jack in the lobby and is able to connect to the company's network. Which of the following should be configured on the existing network infrastructure to best prevent this activity?

Options:

A.

Port security

B.

Web application firewall

C.

Transport layer security

D.

Virtual private network

Answer

A

Explanation

Port security is the best solution to prevent unauthorized devices, like a visitor's laptop, from connecting to the company's network. Port security can limit the number of devices that can connect to a network switch port and block unauthorized MAC addresses, effectively stopping unauthorized access attempts.

Web application firewall (WAF) protects against web-based attacks, not unauthorized network access.

Transport Layer Security (TLS) ensures encrypted communication but does not manage physical network access.

Virtual Private Network (VPN) secures remote connections but does not control access through physical network ports.

Questions # 170:

Which of the following must be considered when designing a high-availability network? (Select two).

Options:

- A.
Ease of recovery
- B.
Ability to patch
- C.
Physical isolation
- D.
Responsiveness
- E.
Attack surface



CertsMania

○ F.

Extensible authentication

Answer

A, E

Explanation

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation of critical services and applications. To achieve this goal, a high-availability network must consider two important factors: ease of recovery and attack surface.

Ease of recovery refers to the ability of a network to quickly restore normal functionality after a failure, disruption, or disaster. A high-availability network should have mechanisms such as redundancy, failover, backup, and restore to ensure that any single point of failure does not cause a complete network outage. A high-availability network should also have procedures and policies for incident response, disaster recovery, and business continuity to minimize the impact of any network issue on the organization's operations and reputation.

Attack surface refers to the exposure of a network to potential threats and vulnerabilities. A high-availability network should have measures such as encryption, authentication, authorization, firewall, intrusion detection and prevention, and patch management to protect the network from unauthorized access, data breaches, malware, denial-of-service attacks, and other cyberattacks. A high-availability network should also have processes and tools for risk assessment, threat intelligence, vulnerability scanning, and penetration testing to identify and mitigate any weaknesses or gaps in the network security.

[References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Architecture and Design, pages 164-1651. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4: Architecture and Design, pages 164-1652., , , , , ,]

Questions # 171:

A security analyst is reviewing the following logs about a suspicious activity alert for a user's VPN log-ins. Which of the following malicious activity indicators triggered the alert?

Log Summary:

User logs in from Chicago, IL multiple times, then suddenly a successful login appears from Rome, Italy, followed again by Chicago logins — all within a short time span.

Options:

A.

Impossible travel

B.

Account lockout

C.

Blocked content

D.

Concurrent session usage



CertsMania

Answer

A

Explanation

Impossible travel (A) refers to logins from geographically distant locations within a time period that makes travel between them physically impossible. In this case, a user logging in from Chicago and Rome within a short time frame triggers this anomaly.

This is a strong indicator of a compromised account or stolen credentials being used elsewhere.

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Indicators of malicious activity: Impossible travel (geolocation anomalies).", , , , ,]

Questions # 172:

A security analyst determines that a security breach will have a financial impact of \$15,000 and is expected to occur twice within a three-year period. Which of the following is the ALE for this risk?

Options:

A.

\$7,500

B.



CertsMania

\$10,000

C.

\$15,000

D.

\$30,000



CertsMania

Answer

B

Explanation

The correct answer is \$10,000 because Annualized Loss Expectancy (ALE) represents the expected yearly financial loss from a specific risk. According to Security+ SY0-701 risk management principles, ALE is calculated using the formula:

$$\text{ALE} = \text{Single Loss Expectancy (SLE)} \times \text{Annualized Rate of Occurrence (ARO)}$$

In this scenario, the Single Loss Expectancy (SLE) is clearly defined as \$15,000, which represents the financial impact of a single security breach. The challenge lies in determining the Annualized Rate of Occurrence (ARO). The breach is expected to occur twice over a three-year period, which means the ARO is:

$$\text{ARO} = 2 \div 3 \approx 0.67 \text{ occurrences per year}$$

Using the ALE formula:

$$\text{ALE} = \$15,000 \times 0.67 \approx \$10,000$$

This calculation aligns with standard quantitative risk assessment techniques emphasized in the SY0-701 study guide. ALE allows organizations to compare the cost of potential losses against the cost of implementing security controls, helping leadership make informed, financially sound risk management decisions.

Option A, \$7,500, would be correct only if the event occurred once every two years. Option C, \$15,000, reflects the SLE but does not account for frequency. Option D, \$30,000, incorrectly represents the total loss over three years rather than an annualized value.

The SY0-701 objectives highlight ALE as a critical metric for prioritizing risks, justifying security investments, and communicating risk in business terms to executives. By converting risk into an annual expected cost, ALE bridges the gap between technical security concerns and organizational financial planning.

In summary, when frequency is spread across multiple years, the loss must be annualized. Doing so correctly results in an ALE of \$10,000, making option B the correct answer.

Questions # 173:

Which of the following threat actors would most likely deface the website of a high-profile music group?

Options:

- A.
Unskilled attacker
- B.
Organized crime
- C.
Nation-state
- D.
Insider threat



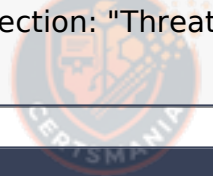
CertsMania

Answer

A

Explanation

Detailed Explanation: An unskilled attacker, often referred to as a script kiddie, is likely to engage in website defacement. This type of attack typically requires minimal expertise and is often conducted for notoriety. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Threat Actors and Motivations".



CertsMania

Questions # 174:

An organization plans to expand its operations internationally and needs to keep data at the new location secure. The organization wants to use the most secure architecture model possible. Which of the following models offers the highest level of security?

Options:

- A.

Cloud-based

B.

Peer-to-peer

C.

On-premises

D.

Hybrid



CertsMania

Answer

A

Explanation

Cloud-based models provide strong security with features like encryption, redundancy, and disaster recovery, making it a secure choice for international operations.

=====

Questions # 175:

A systems administrator creates a script that validates OS version, patch levels, and installed applications when users log in. Which of the following examples best describes the purpose of this script?

Options:

A.

Resource scaling

B.

Policy enumeration

C.

Baseline enforcement

D.



CertsMania

Guardrails implementation

Answer

C

Explanation

Detailed Explanation:

Baseline enforcement ensures that all systems adhere to predefined security configurations, such as approved OS versions and patch levels, improving compliance and reducing vulnerabilities. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "System Baselines and Monitoring".

Questions # 176:

Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

Options:

A.

Jailbreaking

B.

Memory injection

C.

Resource reuse

D.

Side loading

Answer

D

Explanation

Side loading is the process of installing software outside of a manufacturer's approved software repository. This can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access. Side loading can also bypass security controls and policies that are enforced by the manufacturer or the organization. Side loading is often done by users who want to access applications or features that are not available or allowed on their devices. References = Sideloaded - CompTIA Security + Video Training | Interface Technical Training, Security+ (Plus) Certification | CompTIA IT Certifications, Load Balancers - CompTIA Security+ SY0-501 - 2.1, CompTIA Security+ SY0-601 Certification Study Guide.



Questions # 177:

Which of the following should be used to prevent changes to system-level data?

Options:

A.

NIDS

B.

DLP

C.

NAC

D.

FIM



Answer

D

Explanation

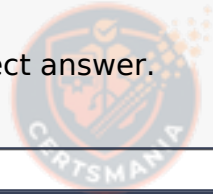
File Integrity Monitoring (FIM) is specifically designed to detect and prevent unauthorized changes to critical system files, configuration files, registry entries, binaries, and logs. According to CompTIA Security+ SY0-701, FIM creates a cryptographic baseline (usually via hashing) of protected system files. Any attempt to modify, add, or delete protected files immediately triggers an alert, enabling rapid detection of tampering—whether caused by malware, insider threats, or misconfigurations.

NIDS (A) monitors network traffic, not system-level modifications. DLP (B) prevents

unauthorized data exfiltration, not system-file tampering. NAC (C) controls device access to the network but does not protect system files.

FIM is a core tool for ensuring system integrity in compliance frameworks such as PCI-DSS, which explicitly requires organizations to monitor critical system files. By preventing unauthorized changes to system-level data and alerting administrators to suspicious activity, FIM provides a strong defensive mechanism against malware, ransomware, and configuration drift.

Thus, FIM is the correct answer.



CertsMania

Questions # 178:

A company has a website in a server cluster. One server is experiencing very high usage, while others are nearly unused. Which of the following should the company configure to help distribute traffic quickly?

Options:

A.

Server multiprocessing

B.

Warm site

C.

Load balancer

D.

Proxy server



CertsMania

Answer

C

Explanation

Comprehensive and Detailed In-Depth Explanation:

A load balancer distributes incoming traffic evenly across multiple servers to prevent any single server from becoming overloaded. This ensures high availability, scalability, and optimal performance of the company's website.

Server multiprocessing (A) refers to the use of multiple processors within a single server but does not distribute traffic across multiple servers.

A warm site (B) is a disaster recovery strategy, not a method for balancing real-time traffic.

A proxy server (D) acts as an intermediary between users and web services but does not distribute server load.

Using a load balancer allows for efficient traffic management and prevents server overload.

Questions # 179:

During a security incident, the security operations team identified sustained network traffic from a malicious IP address:

10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

Options:

A.

access-list inbound deny ig source 0.0.0.0/0 destination 10.1.4.9/32

B.

access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0

C.

access-list inbound permit ig source 10.1.4.9/32 destination 0.0.0.0/0

D.

access-list inbound permit ig source 0.0.0.0/0 destination 10.1.4.9/32

Answer

B

Explanation

A firewall rule is a set of criteria that determines whether to allow or deny a packet to pass through the firewall. A firewall rule consists of several elements, such as the action, the protocol, the source address, the destination address, and the port number. The syntax of a firewall rule may vary depending on the type and vendor of the firewall, but

the basic logic is the same. In this question, the security analyst is creating an inbound firewall rule to block the IP address 10.1.4.9 from accessing the organization's network. This means that the action should be deny, the protocol should be any (or ig for IP), the source address should be 10.1.4.9/32 (which means a single IP address), the destination address should be 0.0.0.0/0 (which means any IP address), and the port number should be any. Therefore, the correct firewall rule is:

```
access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
```

This rule will match any packet that has the source IP address of 10.1.4.9 and drop it. The other options are incorrect because they either have the wrong action, the wrong source address, or the wrong destination address. For example, option A has the source and destination addresses reversed, which means that it will block any packet that has the destination IP address of 10.1.4.9, which is not the intended goal. Option C has the wrong action, which is permit, which means that it will allow the packet to pass through the firewall, which is also not the intended goal. Option D has the same problem as option A, with the source and destination addresses reversed.

References = Firewall Rules - CompTIA Security+ SY0-401: 1.2, Firewalls - SY0-601 CompTIA Security+ : 3.3, Firewalls - CompTIA Security+ SY0-501, Understanding Firewall Rules - CompTIA Network+ N10-005: 5.5, Configuring Windows Firewall - CompTIA A+ 220-1102 - 1.6.

Questions # 180:

Which of the following activities is included in the post-incident review phase?

Options:

A.

Determining the root cause of the incident

B.

Developing steps to mitigate the risks of the incident

C.

Validating the accuracy of the evidence collected during the investigation

D.

Reestablishing the compromised system's configuration and settings

Answer

A

Questions # 181:

A company wants to ensure employees are allowed to copy files from a virtual desktop during the workday but are restricted during non-working hours. Which of the following security measures should the company set up?

Options:

A.

Digital rights management

B.

Role-based access control

C.

Time-based access control

D.

Network access control

Answer

C



CertsMania

To Get Premium Files for SY0-701 Visit

<https://www.certsmania.com/comptia/sy0-701-practice>

For More Free Questions Visit

<https://www.certsmania.com/comptia/pdf/sy0-701>



CertsMania