CompTIA

Exam Questions SY0-701

CompTIA Security+ Exam

NEW QUESTION 1
Which of the following must be considered when designing a high-availability network? (Choose two).

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

Answer: AE

Explanation:
A high-availability network is a network that is designed to minimize downtime and ensure continuous operation even in the event of a failure or disruption. A high-availability network must consider the following factors12:
? Ease of recovery: This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.
? Attack surface: This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening.
The other options are not directly related to high-availability network design:
? Ability to patch: This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.
? Physical isolation: This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network, but it can also reduce the availability and accessibility of the network resources.
? Responsiveness: This refers to the speed and quality of the network's performance and service delivery. Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss. Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.
? Extensible authentication: This refers to the ability of the network to support multiple and flexible authentication methods and protocols. Extensible authentication can improve the security and convenience of the network, but it is not a specific factor for high-availability network design.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability – CompTIA Security+ SY0-701 – 3.4, video by Professor Messer.

NEW QUESTION 2
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?

A. RDP server
B. Jump server
C. Proxy server
D. Hypervisor

Answer: B

Explanation:
= 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.

NEW QUESTION 3
An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?

A. Compromise
B. Retention
C. Analysis
D. Transfer
E. Inventory

Answer: B

Explanation:
A data retention policy is a set of rules that defines how long data should be stored and when it should be deleted or archived. An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period by following the data retention policy of the organization. This policy helps the organization to comply with legal and regulatory requirements, optimize storage space, and protect data privacy and security.
References
? CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, Section 3.4, page 1211
? CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 3, Question 15, page 832

NEW QUESTION 4
Which of the following would be best suited for constantly changing environments?

A. RTOS
B. Containers
C. Embedded systems

D. SCADA

Answer: B

Explanation:
Containers are a method of virtualization that allows applications to run in isolated environments with their own dependencies, libraries, and configurations. Containers are best suited for constantly changing environments because they are lightweight, portable, scalable, and easy to deploy and update. Containers can also support microservices architectures, which enable faster and more frequent delivery of software features. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 512 1

NEW QUESTION 5
A security analyst locates a potentially malicious video file on a server and needs to identify both the creation date and the file's creator. Which of the following actions would most likely give the security analyst the information required?

A. Obtain the file's SHA-256 hash.
B. Use hexdump on the file's contents.
C. Check endpoint logs.
D. Query the file's metadata.

Answer: D

Explanation:
Metadata is data that describes other data, such as its format, origin, creation date, author, and other attributes. Video files, like other types of files, can contain metadata that can provide useful information for forensic analysis. For example, metadata can reveal the camera model, location, date and time, and software used to create or edit the video file. To query the file’s metadata, a security analyst can use various tools, such as MediaInfo1, ffprobe2, or hexdump3, to extract and display the metadata from the video file. By querying the file’s metadata, the security analyst can most likely identify both the creation date and the file’s creator, as well as other relevant information. Obtaining the file’s SHA-256 hash, checking endpoint logs, or using hexdump on the file’s contents are other possible actions, but they are not the most appropriate to answer the question. The file’s SHA-256 hash is a cryptographic value that can be used to verify the integrity or uniqueness of the file, but it does not reveal any information about the file’s creation date or creator. Checking endpoint logs can provide some clues about the file’s origin or activity, but it may not be reliable or accurate, especially if the logs are tampered with or incomplete. Using hexdump on the file’s contents can show the raw binary data of the file, but it may not be easy or feasible to interpret the metadata from the hex output, especially if the file is large or encrypted. References: 1: How do I get the meta-data of a video file? 2: How to check if an mp4 file contains malware? 3: [Hexdump - Wikipedia]

NEW QUESTION 6
Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

A. Risk tolerance
B. Risk transfer
C. Risk register
D. Risk analysis

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.

NEW QUESTION 7
Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?

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

NEW QUESTION 8
A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?

A. Patch availability
B. Product software compatibility
C. Ease of recovery
D. Cost of replacement

Answer: A

Explanation:
End-of-life operating systems are those that are no longer supported by the vendor or manufacturer, meaning they do not receive any security updates or patches. This makes them vulnerable to exploits and attacks that take advantage of known or unknown flaws in the software. Patch availability is the security implication of using end-of-life operating systems, as it affects the ability to fix or prevent security issues. Other factors, such as product software compatibility, ease of recovery, or cost of replacement, are not directly related to security, but rather to functionality, availability, or budget. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 29 1

NEW QUESTION 9
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?

A. Default credentials
B. Non-segmented network
C. Supply chain vendor
D. Vulnerable software

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.

NEW QUESTION 10
A security administrator needs a method to secure data in an environment that includes some form of checks so that the administrator can track any changes. Which of the following should the administrator set up to achieve this goal?

A. SPF
B. GPO
C. NAC
D. FIM

Answer: D

Explanation:
FIM stands for File Integrity Monitoring, which is a method to secure data by detecting any changes or modifications to files, directories, or registry keys. FIM can help a security administrator track any unauthorized or malicious changes to the data, as well as verify the integrity and compliance of the data. FIM can also alert the administrator of any potential breaches or incidents involving the data.
Some of the benefits of FIM are:
? It can prevent data tampering and corruption by verifying the checksums or hashes of the files.
? It can identify the source and time of the changes by logging the user and system actions.
? It can enforce security policies and standards by comparing the current state of the data with the baseline or expected state.
? It can support forensic analysis and incident response by providing evidence and audit trails of the changes.
References:
? CompTIA Security+ SY0-701 Certification Study Guide, Chapter 5: Technologies and Tools, Section 5.3: Security Tools, p. 209-210
? CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 2: Technologies and Tools, Objective 2.4: Given a scenario, analyze and interpret output from security technologies, Sub-objective: File integrity monitor, p. 12

NEW QUESTION 10
Which of the following exercises should an organization use to improve its incident response process?

A. Tabletop
B. Replication
C. Failover
D. Recovery

Answer: A

Explanation:
A tabletop exercise is a simulated scenario that tests the organization’s incident response plan and procedures. It involves key stakeholders and decision-makers who discuss their roles and actions in response to a hypothetical incident. It can help identify gaps, weaknesses, and improvement areas in the incident response process. It can also enhance communication, coordination, and collaboration among the
participants. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 525 1

NEW QUESTION 15
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?

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.

NEW QUESTION 18
Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?

A. Configure all systems to log scheduled tasks.
B. Collect and monitor all traffic exiting the network.
C. Block traffic based on known malicious signatures.
D. Install endpoint management software on all systems.

Answer: D

Explanation:
Endpoint management software is a tool that allows security engineers to monitor and control the configuration, security, and performance of workstations and servers from a central console. Endpoint management software can help detect and prevent unauthorized changes and software installations, enforce policies and compliance, and provide reports and alerts on the status of the endpoints. The other options are not as effective or comprehensive as endpoint management software for this
purpose. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page
137 1

NEW QUESTION 20
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?

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.

NEW QUESTION 21
A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

A. Password spraying
B. Account forgery
C. Pass-t he-hash
D. Brute-force

Answer: A

Explanation:
Password spraying is a type of brute force attack that tries common passwords across several accounts to find a match. It is a mass trial-and-error approach that can bypass account lockout protocols. It can give hackers access to personal or business accounts and information. It is not a targeted attack, but a high-volume attack tactic that uses a dictionary or a list of popular or weak passwords12.
The logs show that the attacker is using the same password ("password123") to attempt to log in to different accounts ("admin", "user1", "user2", etc.) on the same web server. This is a typical pattern of password spraying, as the attacker is hoping that at least one of the accounts has a weak password that matches the one they are trying. The attacker is also using a tool called Hydra, which is one of the most popular brute force tools, often used in cracking passwords for network authentication3.
Account forgery is not the correct answer, because it involves creating fake accounts or credentials to impersonate legitimate users or entities. There is no evidence of account forgery in the logs, as the attacker is not creating any new accounts or using forged credentials.
Pass-the-hash is not the correct answer, because it involves stealing a hashed user credential and using it to create a new authenticated session on the same

network. Pass- the-hash does not require the attacker to know or crack the password, as they use the stored version of the password to initiate a new session4. The logs show that the attacker is using plain text passwords, not hashes, to try to log in to the web server.
Brute-force is not the correct answer, because it is a broader term that encompasses different types of attacks that involve trying different variations of symbols or words until the correct password is found. Password spraying is a specific type of brute force attack that uses a single common password against multiple accounts5. The logs show that the attacker is using password spraying, not brute force in general, to try to gain access to the web server. References = 1: Password spraying: An overview of password spraying attacks … - Norton, 2: Security: Credential Stuffing vs. Password Spraying - Baeldung, 3: Brute Force Attack: A definition + 6 types to know | Norton, 4: What is a Pass- the-Hash Attack? - CrowdStrike, 5: What is a Brute Force Attack? | Definition, Types & How It Works - Fortinet

NEW QUESTION 24
A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

A. The user jsmith's account has been locked out.
B. A keylogger is installed on [smith's workstation
C. An attacker is attempting to brute force ismith's account.
D. Ransomware has been deployed in the domain.

Answer: C

Explanation:
Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tools or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user ismith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of ismith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset ismith's password, and notify ismith of the incident. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2. Threat Actors and Attributes – SY0-601 CompTIA Security+ : 1.1

NEW QUESTION 28
One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update. Which of the following vulnerability types is being addressed by the patch?

A. Virtualization
B. Firmware
C. Application
D. Operating system

Answer: B

Explanation:
Firmware is a type of software that is embedded in hardware devices, such as BIOS, routers, printers, or cameras. Firmware controls the basic functions and operations of the device, and can be updated or patched to fix bugs, improve performance, or enhance security. Firmware vulnerabilities are flaws or weaknesses in the firmware code that can be exploited by attackers to gain unauthorized access, modify settings, or cause damage to the device or the network. A BIOS update is a patch that addresses a firmware vulnerability in the basic input/output system of a computer, which is responsible for booting the operating system and managing the communication between the hardware and the software. The other options are not types of vulnerabilities, but rather categories of software or technology.

NEW QUESTION 29
A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

A. Packet captures
B. Vulnerability scans
C. Metadata
D. Dashboard

Answer: D

Explanation:
A dashboard is a graphical user interface that provides a visual representation of key performance indicators, metrics, and trends related to security events and incidents. A dashboard can help the board of directors to understand the number and impact of incidents that affected the organization in a given period, as well as the status and effectiveness of the security controls and processes. A dashboard can also allow the board of directors to drill down into specific details or filter the data by various criteria12.
A packet capture is a method of capturing and analyzing the network traffic that passes through a device or a network segment. A packet capture can provide detailed information about the source, destination, protocol, and content of each packet, but it is not a suitable way to present a summary of incidents to the board of directors13.
A vulnerability scan is a process of identifying and assessing the weaknesses and exposures in a system or a network that could be exploited by attackers. A vulnerability scan can help the organization to prioritize and remediate the risks and improve the security posture, but it is not a relevant way to report the number of incidents that occurred in a quarter14.
Metadata is data that describes other data, such as its format, origin, structure, or context. Metadata can provide useful information about the characteristics and properties of data, but it is not a meaningful way to communicate the impact and frequency of incidents to the board of directors. References = 1: CompTIA

Security+ SY0-701 Certification Study Guide, page 3722: SIEM Dashboards – SY0-601 CompTIA Security+ : 4.3, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 3464: CompTIA Security+ SY0-701 Certification Study Guide, page 362. : CompTIA Security+ SY0-701 Certification Study Guide, page 97.

NEW QUESTION 30
After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

A. Retain the emails between the security team and affected customers for 30 days.
B. Retain any communications related to the security breach until further notice.
C. Retain any communications between security members during the breach response.
D. Retain all emails from the company to affected customers for an indefinite period of time.

Answer: B

Explanation:
A legal hold (also known as a litigation hold) is a notification sent from an organization’s legal team to employees instructing them not to delete electronically stored information (ESI) or discard paper documents that may be relevant to a new or imminent legal case. A legal hold is intended to preserve evidence and prevent spoliation, which is the intentional or negligent destruction of evidence that could harm a party’s case. A legal hold can be triggered by various events, such as a lawsuit, a regulatory investigation, or a subpoena12 In this scenario, the company’s attorneys have requested that the security team initiate a legal hold in response to the lawsuit filed by the customers after the company was compromised. This means that the security team will most likely be required to retain any communications related to the security breach until further notice. This could include emails, instant messages, reports, logs, memos, or any other documents that could be relevant to the lawsuit. The security team should also inform the relevant custodians (the employees who have access to or control over the ESI) of their preservation obligations and monitor their compliance. The security team should also document the legal hold process and its scope, as well as take steps to protect the ESI from alteration, deletion, or loss34
References:
1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 303 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 305 3: Legal Hold (Litigation Hold) - The Basics of E-Discovery - Exterro 5 4: The Legal Implications and Consequences of a Data Breach 6

NEW QUESTION 31
A systems administrator receives the following alert from a file integrity monitoring tool: The hash of the cmd.exe file has changed.
The systems administrator checks the OS logs and notices that no patches were applied in the last two months. Which of the following most likely occurred?

A. The end user changed the file permissions.
B. A cryptographic collision was detected.
C. A snapshot of the file system was taken.
D. A rootkit was deployed.

Answer: D

Explanation:
A rootkit is a type of malware that modifies or replaces system files or processes to hide its presence and activity. A rootkit can change the hash of the cmd.exe file, which is a command-line interpreter for Windows systems, to avoid detection by antivirus or file integrity monitoring tools. A rootkit can also grant the attacker remote access and control over the infected system, as well as perform malicious actions such as stealing data, installing backdoors, or launching attacks on other systems. A rootkit is one of the most difficult types of malware to remove, as it can persist even after rebooting or
reinstalling the OS. References = CompTIA Security+ Study Guide with over 500 Practice
Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 147. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2, page 9.

NEW QUESTION 36
Which of the following scenarios describes a possible business email compromise attack?

A. An employee receives a gift card request in an email that has an executive's name in the display field of the email.
B. Employees who open an email attachment receive messages demanding payment in order to access files.
C. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
D. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Answer: A

Explanation:
A business email compromise (BEC) attack is a type of phishing attack that targets employees who have access to company funds or sensitive information. The attacker impersonates a trusted person, such as an executive, a vendor, or a client, and requests a fraudulent payment, a wire transfer, or confidential data. The attacker often uses social engineering techniques, such as urgency, pressure, or familiarity, to convince the victim to comply with the request12.
In this scenario, option A describes a possible BEC attack, where an employee receives a gift card request in an email that has an executive’s name in the display field of the email. The email may look like it is coming from the executive, but the actual email address may be spoofed or compromised. The attacker may claim that the gift cards are needed for a business purpose, such as rewarding employees or clients, and ask the employee to purchase them and send the codes. This is a common tactic used by BEC attackers to steal money from unsuspecting victims34.
Option B describes a possible ransomware attack, where malicious software encrypts the files on a device and demands a ransom for the decryption key. Option C describes a possible credential harvesting attack, where an attacker tries to obtain the login information of a privileged account by posing as a legitimate authority. Option D describes a possible phishing attack, where an attacker tries to lure the victim to a fake website that mimics the company’s email portal and capture their credentials. These are all types of cyberattacks, but they are not examples of BEC attacks. References = 1: Business Email Compromise - CompTIA Security+ SY0-701 - 2.2 2: CompTIA Security+ SY0-701 Certification Study Guide 3: Business Email Compromise: The 12 Billion Dollar Scam 4: TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy

NEW QUESTION 41
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?

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:
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

NEW QUESTION 44
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?

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.

NEW QUESTION 46
A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation. Which of the following logs should the analyst use as a data source?

A. Application
B. IPS/IDS
C. Network
D. Endpoint

Answer: D

Explanation:
An endpoint log is a file that contains information about the activities and events that occur on an end-user device, such as a laptop, desktop, tablet, or smartphone. Endpoint logs can provide valuable data for security analysts, such as the processes running on the device, the network connections established, the files accessed or modified, the user actions performed, and the applications installed or updated. Endpoint logs can also record the details of any executable files running on the device, such as the name, path, size, hash, signature, and permissions of the executable.
An application log is a file that contains information about the events that occur within a software application, such as errors, warnings, transactions, or performance metrics. Application logs can help developers and administrators troubleshoot issues, optimize performance, and monitor user behavior. However, application logs may not provide enough information about the executable files running on the device, especially if they are malicious or unknown.
An IPS/IDS log is a file that contains information about the network traffic that is monitored and analyzed by an intrusion prevention system (IPS) or an intrusion detection system (IDS). IPS/IDS logs can help security analysts identify and block potential attacks, such as exploit attempts, denial-of-service (DoS) attacks, or malicious scans. However, IPS/IDS logs may not provide enough information about the executable files running on the device, especially if they are encrypted, obfuscated, or use legitimate protocols.
A network log is a file that contains information about the network activity and communication that occurs between devices, such as IP addresses, ports, protocols, packets, or bytes. Network logs can help security analysts understand the network topology, traffic patterns, and bandwidth usage. However, network logs may not provide enough information about the executable files running on the device, especially if they are hidden, spoofed, or use proxy servers.
Therefore, the best log type to use as a data source for additional information about the executable running on the machine is the endpoint log, as it can provide the most relevant and detailed data about the executable file and its behavior.
References = https://www.crowdstrike.com/cybersecurity-101/observability/application-log/
https://owasp.org/www-project-proactive-controls/v3/en/c9-security-logging

NEW QUESTION 47
A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

A. Place posters around the office to raise awareness of common phishing activities.
B. Implement email security filters to prevent phishing emails from being delivered
C. Update the EDR policies to block automatic execution of downloaded programs.

D. Create additional training for users to recognize the signs of phishing attempts.

Answer: C

Explanation:
An endpoint detection and response (EDR) system is a security tool that monitors and analyzes the activities and behaviors of endpoints, such as computers, laptops, mobile devices, and servers. An EDR system can detect, prevent, and respond to various types of threats, such as malware, ransomware, phishing, and advanced persistent threats (APTs). One of the features of an EDR system is to block the automatic execution of downloaded programs, which can prevent malicious code from running on the endpoint when a user clicks on a link in a phishing message. This can reduce the impact of a phishing attack and protect the endpoint from compromise. Updating the EDR policies to block automatic execution of downloaded programs is a technical control that can mitigate the risk of phishing, regardless of the user's awareness or behavior. Therefore, this is the best answer among the given options.
The other options are not as effective as updating the EDR policies, because they rely on administrative or physical controls that may not be sufficient to prevent or stop a phishing attack. Placing posters around the office to raise awareness of common phishing activities is a physical control that can increase the user's knowledge of phishing, but it may not change their behavior or prevent them from clicking on a link in a phishing message. Implementing email security filters to prevent phishing emails from being delivered is an administrative control that can reduce the exposure to phishing, but it may not be able to block all phishing emails, especially if they are crafted to bypass the filters. Creating additional training for users to recognize the signs of phishing attempts is an administrative control that can improve the user's skills of phishing detection, but it may not guarantee that they will always be vigilant or cautious when receiving an email. Therefore, these options are not the best answer for this question. References = Endpoint Detection and Response – CompTIA Security+ SY0-701 – 2.2, video at 5:30; CompTIA Security+ SY0- 701 Certification Study Guide, page 163.

NEW QUESTION 50
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?

A. Smishing
B. Disinformation
C. Impersonating
D. Whaling

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.

NEW QUESTION 52
Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

A. SCAP
B. Net Flow
C. Antivirus
D. DLP

Answer: D

Explanation:
DLP stands for Data Loss Prevention, which is a tool that can assist with detecting and preventing the unauthorized transmission or leakage of sensitive data, such as a customer's PII (Personally Identifiable Information). DLP can monitor, filter, and block data in motion (such as emails), data at rest (such as files), and data in use (such as applications). DLP can also alert the sender, the recipient, or the administrator of the data breach, and apply remediation actions, such as encryption, quarantine, or deletion. DLP can help an organization comply with data protection regulations, such as GDPR, HIPAA, or PCI DSS, and protect its reputation and assets. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 78. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.5, page 11.

NEW QUESTION 54
A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

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

Answer: D

Explanation:
Ransomware-as-a-service is a type of cybercrime where hackers sell or rent ransomware tools or services to other criminals who use them to launch attacks and extort money from victims. This is a typical example of organized crime, which is a group of criminals who work together to conduct illegal activities for profit. Organized crime is different from other types of threat actors, such as insider threats, hacktivists, or nation-states, who may have different motives, methods, or targets. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17 1

NEW QUESTION 59
Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?

A. Software as a service
B. Infrastructure as code
C. Internet of Things
D. Software-defined networking

Answer: B

Explanation:
Infrastructure as code (IaC) is a method of using code and automation to manage and provision cloud resources, such as servers, networks, storage, and applications. IaC allows for easy deployment, scalability, consistency, and repeatability of cloud environments. IaC is also a key component of DevSecOps, which integrates security into the development and operations processes. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Cloud and Virtualization Concepts, page 294.

NEW QUESTION 63
A systems administrator is looking for a low-cost application-hosting solution that is cloud- based. Which of the following meets these requirements?

A. Serverless framework
B. Type 1 hvpervisor
C. SD-WAN
D. SDN

Answer: A

Explanation:
A serverless framework is a cloud-based application-hosting solution that meets the requirements of low-cost and cloud-based. A serverless framework is a type of cloud computing service that allows developers to run applications without managing or provisioning any servers. The cloud provider handles the server-side infrastructure, such as scaling, load balancing, security, and maintenance, and charges the developer only for the resources consumed by the application. A serverless framework enables developers to focus on the application logic and functionality, and reduces the operational costs and complexity of hosting applications. Some examples of serverless frameworks are AWS Lambda, Azure Functions, and Google Cloud Functions.
A type 1 hypervisor, SD-WAN, and SDN are not cloud-based application-hosting solutions that meet the requirements of low-cost and cloud-based. A type 1 hypervisor is a software layer that runs directly on the hardware and creates multiple virtual machines that can run different operating systems and applications. A type 1 hypervisor is not a cloud-based service, but a virtualization technology that can be used to create private or hybrid clouds. A type 1 hypervisor also requires the developer to manage and provision the servers and the virtual machines, which can increase the operational costs and complexity of hosting applications. Some examples of type 1 hypervisors are VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.
SD-WAN (Software-Defined Wide Area Network) is a network architecture that uses software to dynamically route traffic across multiple WAN connections, such as broadband, LTE, or MPLS. SD-WAN is not a cloud-based service, but a network optimization technology that can improve the performance, reliability, and security of WAN connections. SD-WAN can be used to connect remote sites or users to cloud-based applications, but it does not host the applications itself. Some examples of SD-WAN vendors are Cisco, VMware, and Fortinet.
SDN (Software-Defined Networking) is a network architecture that decouples the control plane from the data plane, and uses a centralized controller to programmatically manage and configure the network devices and traffic flows. SDN is not a cloud-based service, but a network automation technology that can enhance the scalability, flexibility, and efficiency of the network. SDN can be used to create virtual networks or network functions that can support cloud-based applications, but it does not host the applications itself. Some examples of SDN vendors are OpenFlow, OpenDaylight, and OpenStack.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 264-265; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 7:40 - 10:00; [Serverless Framework]; [Type 1 Hypervisor]; [SD-WAN]; [SDN].

NEW QUESTION 67
Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company?

A. Provisioning resources
B. Disabling access
C. Reviewing change approvals
D. Escalating permission requests

Answer: B

Explanation:
Disabling access is an automation use case that would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company. Disabling access is the process of revoking or suspending the access rights of a user account, such as login credentials, email, VPN, cloud services, etc. Disabling access can prevent unauthorized or malicious use of the account by former employees or attackers who may have compromised the account. Disabling access can also reduce the attack surface and the risk of data breaches or leaks. Disabling access can be automated by using scripts, tools, or workflows that can trigger the action based on predefined events, such as employee termination, resignation, or transfer. Automation can ensure that the access is disabled in a timely, consistent, and efficient manner, without relying on manual intervention or human error.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Identity and Access Management, page 2131. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5: Identity and Access Management, page 2132.

NEW QUESTION 72
Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

A. Preparation
B. Recovery
C. Lessons learned
D. Analysis

Answer: A

Explanation:
Preparation is the phase in the incident response process when a security analyst reviews roles and responsibilities, as well as the policies and procedures for handling incidents. Preparation also involves gathering and maintaining the necessary tools, resources, and contacts for responding to incidents. Preparation can help a security analyst to be ready and proactive when an incident occurs, as well as to reduce the impact and duration of the incident.
Some of the activities that a security analyst performs during the preparation phase are:
? Defining the roles and responsibilities of the incident response team members, such as the incident manager, the incident coordinator, the technical lead, the communications lead, and the legal advisor.
? Establishing the incident response plan, which outlines the objectives, scope, authority, and procedures for responding to incidents, as well as the escalation and reporting mechanisms.

? Developing the incident response policy, which defines the types and categories of incidents, the severity levels, the notification and reporting requirements, and the roles and responsibilities of the stakeholders.
? Creating the incident response playbook, which provides the step-by-step guidance and checklists for handling specific types of incidents, such as denial-of-service, ransomware, phishing, or data breach.
? Acquiring and testing the incident response tools, such as network and host-based scanners, malware analysis tools, forensic tools, backup and recovery tools, and communication and collaboration tools.
? Identifying and securing the incident response resources, such as the incident response team, the incident response location, the evidence storage, and the external support.
? Building and maintaining the incident response contacts, such as the internal and external stakeholders, the law enforcement agencies, the regulatory bodies, and the media.
References:
? CompTIA Security+ SY0-701 Certification Study Guide, Chapter 6: Architecture and Design, Section 6.4: Secure Systems Design, p. 279-280
? CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.5: Given a scenario, implement secure network architecture concepts, Sub-objective: Incident response, p. 16

NEW QUESTION 74
A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done next?

A. Conduct an audit.
B. Initiate a penetration test.
C. Rescan the network.
D. Submit a report.

Answer: C

Explanation:
After completing a vulnerability assessment and remediating the identified vulnerabilities, the next step is to rescan the network to verify that the vulnerabilities have been successfully fixed and no new vulnerabilities have been introduced. A vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network, system, or application that could be exploited by attackers. A vulnerability assessment typically involves using automated tools, such as scanners, to scan the network and generate a report of the findings. The report may include information such as the severity, impact, and remediation of the vulnerabilities. The operations team is responsible for applying the appropriate patches, updates, or configurations to address the vulnerabilities and reduce the risk to the network. A rescan is necessary to confirm that the remediation actions have been effective and that the network is secure.
Conducting an audit, initiating a penetration test, or submitting a report are not the next steps after completing a vulnerability assessment and remediating the vulnerabilities. An audit is a process of reviewing and verifying the compliance of the network with the established policies, standards, and regulations. An audit may be performed by internal or external auditors, and it may use the results of the vulnerability assessment as part of the evidence. However, an audit is not a mandatory step after a vulnerability assessment, and it does not validate the effectiveness of the remediation actions.
A penetration test is a process of simulating a real-world attack on the network to test the security defenses and identify any gaps or weaknesses. A penetration test may use the results of the vulnerability assessment as a starting point, but it goes beyond scanning and involves exploiting the vulnerabilities to gain access or cause damage. A penetration test may be performed after a vulnerability assessment, but only with the proper authorization, scope, and rules of engagement. A penetration test is not a substitute for a rescan, as it does not verify that the vulnerabilities have been fixed.
Submitting a report is a step that is done after the vulnerability assessment, but before the remediation. The report is a document that summarizes the findings and recommendations of the vulnerability assessment, and it is used to communicate the results to the stakeholders and the operations team. The report may also include a follow-up plan and a timeline for the remediation actions. However, submitting a report is not the final step after the remediation, as it does not confirm that the network is secure.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 372- 375; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 0:00 - 8:00.

NEW QUESTION 79
The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

A. Shadow IT
B. Insider threat
C. Data exfiltration
D. Service disruption

Answer: A

Explanation:
Shadow IT is the term used to describe the use of unauthorized or unapproved IT resources within an organization. The marketing department set up its own project management software without telling the appropriate departments, such as IT, security, or compliance. This could pose a risk to the organization's security posture, data integrity, and regulatory compliance1.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 35.

NEW QUESTION 83
Which of the following would be the best way to handle a critical business application that is running on a legacy server?

A. Segmentation
B. Isolation
C. Hardening
D. Decommissioning

Answer: C

Explanation:
A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues. A critical business application is an application that is essential for the operation and continuity of the business, such as accounting, payroll, or inventory management. A legacy server running a critical business application may be difficult to replace or upgrade, but it should not be left unsecured or exposed to potential threats.
One of the best ways to handle a legacy server running a critical business application is to harden it. Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability. Hardening a legacy server may involve steps such as:

? Applying patches and updates to the operating system and the application, if available
? Removing or disabling unnecessary services, features, or accounts
? Configuring firewall rules and network access control lists to restrict inbound and outbound traffic
? Enabling encryption and authentication for data transmission and storage
? Implementing logging and monitoring tools to detect and respond to anomalous or malicious activity
? Performing regular backups and testing of the system and the application Hardening a legacy server can help protect the critical business application from unauthorized access, modification, or disruption, while maintaining its functionality and availability. However, hardening a legacy server is not a permanent solution, and it may not be sufficient to address all the security issues and challenges posed by the outdated or unsupported system. Therefore, it is advisable to plan for the eventual decommissioning or migration of the legacy server to a more secure and modern platform, as soon as possible. References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 3: Architecture and Design, Section 3.2: Secure System Design, Page 133 1; CompTIA Security+ Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.2: Explain the importance of secure system design, Subobjective: Legacy systems 2

NEW QUESTION 86
Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

A. Key stretching
B. Data masking
C. Steganography
D. Salting

Answer: D

Explanation:
Salting is the process of adding extra random data to a password or other data before applying a one-way data transformation algorithm, such as a hash function. Salting increases the complexity and randomness of the input data, making it harder for attackers to guess or crack the original data using precomputed tables or brute force methods. Salting also helps prevent identical passwords from producing identical hash values, which could reveal the passwords to attackers who have access to the hashed data. Salting is commonly used to protect passwords stored in databases or transmitted over networks. References =
? Passwords technical overview
? Encryption, hashing, salting – what's the difference?
? Salt (cryptography)

NEW QUESTION 88
Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?

A. Automation
B. Compliance checklist
C. Attestation
D. Manual audit

Answer: A

Explanation:
Automation is the best way to consistently determine on a daily basis whether security settings on servers have been modified. Automation is the process of using software, hardware, or other tools to perform tasks that would otherwise require human intervention or manual effort. Automation can help to improve the efficiency, accuracy, and consistency of security operations, as well as reduce human errors and costs. Automation can be used to monitor, audit, and enforce security settings on servers, such as firewall rules, encryption keys, access controls, patch levels, and configuration files. Automation can also alert security personnel of any changes or anomalies that may indicate a security breach or compromise12.
The other options are not the best ways to consistently determine on a daily basis whether security settings on servers have been modified:
? Compliance checklist: This is a document that lists the security requirements, standards, or best practices that an organization must follow or adhere to. A compliance checklist can help to ensure that the security settings on servers are aligned with the organizational policies and regulations, but it does not automatically detect or report any changes or modifications that may occur on a daily basis3.
? Attestation: This is a process of verifying or confirming the validity or accuracy of a statement, claim, or fact. Attestation can be used to provide assurance or evidence that the security settings on servers are correct and authorized, but it does not continuously monitor or audit any changes or modifications that may occur on a daily basis4.
? Manual audit: This is a process of examining or reviewing the security settings on servers by human inspectors or auditors. A manual audit can help to identify and correct any security issues or discrepancies on servers, but it is time-consuming, labor-intensive, and prone to human errors. A manual audit may not be feasible or practical to perform on a daily basis.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: Automation and Scripting – CompTIA Security+ SY0-701 – 5.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 98. : CompTIA Security+ SY0-701 Certification Study Guide, page 99.

NEW QUESTION 90
A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.
Which of the following teams will conduct this assessment activity?

A. White
B. Purple
C. Blue
D. Red

Answer: D

Explanation:
A red team is a group of security professionals who perform offensive security assessments covering penetration testing and social engineering. A red team simulates real-world attacks and exploits the vulnerabilities of a target organization, system, or network. A red team aims to test the effectiveness of the security controls, policies, and procedures of the target, as well as the awareness and response of the staff and the blue team. A red team can be hired as an external consultant or formed internally within the organization. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 18. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.8, page 4. Security Teams – SY0-601 CompTIA Security+ : 1.8

NEW QUESTION 92
Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

A. Integrity
B. Availability
C. Confidentiality
D. Non-repudiation

Answer: C

Explanation:
Confidentiality is the security concept that ensures data is protected from unauthorized access or disclosure. The principle of least privilege is a technique that grants users or systems the minimum level of access or permissions that they need to perform their tasks, and nothing more. By applying the principle of least privilege to a human resources fileshare, the permissions can be restricted to only those who have a legitimate need to access the sensitive data, such as HR staff, managers, or auditors. This can prevent unauthorized users, such as hackers, employees, or contractors, from accessing, copying, modifying, or deleting the data. Therefore, the principle of least privilege can enhance the confidentiality of the data on the fileshare. Integrity, availability, and non- repudiation are other security concepts, but they are not the best reason for permissions on a human resources fileshare to follow the principle of least privilege. Integrity is the security concept that ensures data is accurate and consistent, and protected from unauthorized modification or corruption. Availability is the security concept that ensures data is accessible and usable by authorized users or systems when needed. Non-repudiation is the security concept that ensures the authenticity and accountability of data and actions, and prevents the denial of involvement or responsibility. While these concepts are also important for data security, they are not directly related to the level of access or permissions granted to users or systems. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17, 372-373

NEW QUESTION 95
Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated:
“I’m in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address.”
Which of the following are the best responses to this situation? (Choose two).

A. Cancel current employee recognition gift cards.
B. Add a smishing exercise to the annual company training.
C. Issue a general email warning to the company.
D. Have the CEO change phone numbers.
E. Conduct a forensic investigation on the CEO's phone.
F. Implement mobile device management.

Answer: BC

Explanation:
This situation is an example of smishing, which is a type of phishing that uses text messages (SMS) to entice individuals into providing personal or sensitive information to cybercriminals. The best responses to this situation are to add a smishing exercise to the annual company training and to issue a general email warning to the company. A smishing exercise can help raise awareness and educate employees on how to recognize and avoid smishing attacks. An email warning can alert employees to the fraudulent text message and remind them to verify the identity and legitimacy of any requests for information or money. References = What Is Phishing | Cybersecurity | CompTIA, Phishing – SY0-601 CompTIA Security+ : 1.1 - Professor Messer IT Certification Training Courses

NEW QUESTION 98
An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

A. Segmentation
B. Isolation
C. Patching
D. Encryption

Answer: A

Explanation:
Segmentation is a network design technique that divides the network into smaller and isolated segments based on logical or physical boundaries. Segmentation can help improve network security by limiting the scope of an attack, reducing the attack surface, and enforcing access control policies. Segmentation can also enhance network performance, scalability, and manageability. To accomplish the goal of storing customer data on a separate part of the network, the administrator can use segmentation technologies such as subnetting, VLANs, firewalls, routers, or switches. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 1

NEW QUESTION 99
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?

A. Guard rail script
B. Ticketing workflow
C. Escalation script
D. User provisioning script

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.

NEW QUESTION 102
A user is attempting to patch a critical system, but the patch fails to transfer. Which of the following access controls is most likely inhibiting the transfer?

A. Attribute-based
B. Time of day
C. Role-based
D. Least privilege

Answer: D

Explanation:
The least privilege principle states that users and processes should only have the minimum level of access required to perform their tasks. This helps to prevent unauthorized or unnecessary actions that could compromise security. In this case, the patch transfer might be failing because the user or process does not have the appropriate permissions to access the critical system or the network resources needed for the transfer. Applying the least privilege principle can help to avoid this issue by granting the user or process the necessary access rights for the patching activity. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 931

NEW QUESTION 104
HOTSPOT
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.
INSTRUCTIONS
Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services

A. Mastered

B. Not Mastered

Answer: A

Explanation:
Web serverBotnet Enable DDoS protectionUser RAT Implement a host-based IPS Database server Worm Change the default application passwordExecutive KeyloggerDisable vulnerable servicesApplication Backdoor Implement 2FA using push notification

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

A screenshot of a computer program
Description automatically generated with low confidence

NEW QUESTION 108
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SY0-701 Practice Exam Features:

* SY0-701 Questions and Answers Updated Frequently

* SY0-701 Practice Questions Verified by Expert Senior Certified Staff

* SY0-701 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SY0-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year