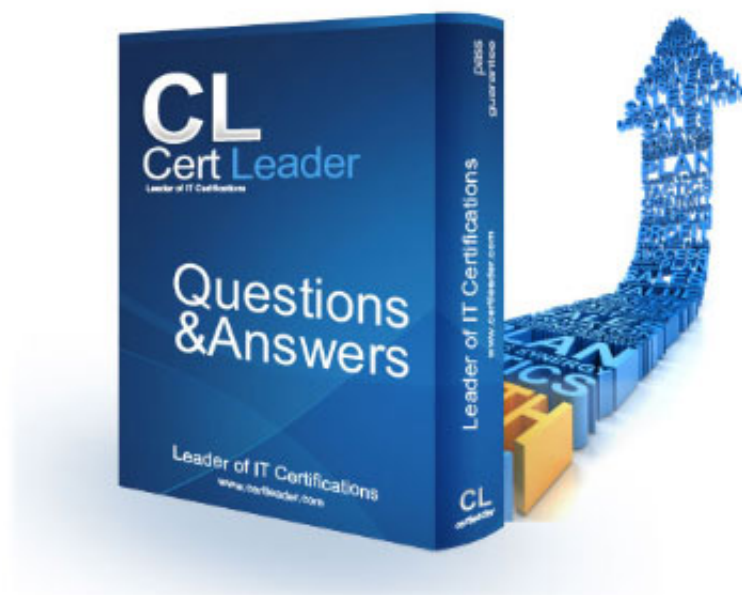


CAS-005 Dumps

CompTIA SecurityX Exam

<https://www.certleader.com/CAS-005-dumps.html>



NEW QUESTION 1

A company's help desk is experiencing a large number of calls from the finance department slating access issues to www.bank.com The security operations center reviewed the following security logs:

User	User IP & Subnet	Location	Website	DNS Resolved IP (public)	HTTP Status Code
User12	10.200.2.52/24	Finance	www.bank.com	65.146.76.34	495
User31	10.200.2.213/24	Finance	www.bank.com	65.146.76.34	495
User46	10.200.5.76/24	IT	www.bank.com	98.17.62.78	200
User23	10.200.2.156/24	Finance	www.bank.com	65.146.76.34	495
User51	10.200.4.138/24	Legal	www.bank.com	98.17.62.78	200

Which of the following is most likely the cause of the issue?

- A. Recursive DNS resolution is failing
- B. The DNS record has been poisoned.
- C. DNS traffic is being sinkholed.
- D. The DNS was set up incorrectly.

Answer: C

Explanation:

Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination. This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.

In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.

? Recursive DNS resolution failure (A) would generally lead to inability to resolve DNS at all, not to a specific HTTP error.

? DNS poisoning (B) could result in users being directed to malicious sites, but again, would likely result in a different set of errors or unusual activity.

? Incorrect DNS setup (D) would likely cause broader resolution issues rather than targeted errors like the one seen here.

By reviewing the provided data, it is evident that the DNS traffic for www.bank.com is being rerouted improperly, resulting in consistent HTTP 495 errors for the finance department users. Hence, the most likely cause is that the DNS traffic is being sinkholed.

References:

? CompTIA SecurityX study materials on DNS security mechanisms.

? Standard HTTP status codes and their implications.

NEW QUESTION 2

Which of the following best explains the business requirement a healthcare provider fulfills by encrypting patient data at rest?

- A. Securing data transfer between hospitals
- B. Providing for non-repudiation data
- C. Reducing liability from identity theft
- D. Protecting privacy while supporting portability.

Answer: D

Explanation:

Encrypting patient data at rest is a critical requirement for healthcare providers to ensure compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The primary business requirement fulfilled by this practice is the protection of patient privacy while supporting the portability of medical information. By encrypting data at rest, healthcare providers safeguard sensitive patient information from unauthorized access, ensuring that privacy is maintained even if the storage media are compromised. Additionally, encryption supports the portability of patient records, allowing for secure transfer and access across different systems and locations while ensuring that privacy controls are in place.

References:

? CompTIA SecurityX Study Guide: Emphasizes the importance of data encryption for protecting sensitive information and ensuring compliance with regulatory requirements.

? HIPAA Security Rule: Requires healthcare providers to implement safeguards, including encryption, to protect patient data.

? "Health Informatics: Practical Guide for Healthcare and Information Technology Professionals" by Robert E. Hoyt: Discusses encryption as a key measure for protecting patient data privacy and supporting data portability.

NEW QUESTION 3

An organization wants to implement a platform to better identify which specific assets are affected by a given vulnerability. Which of the following components provides the best foundation to achieve this goal?

- A. SASE
- B. CMDB
- C. SBoM
- D. SLM

Answer: B

Explanation:

A Configuration Management Database (CMDB) provides the best foundation for identifying which specific assets are affected by a given vulnerability. A CMDB maintains detailed information about the IT environment, including hardware, software, configurations, and relationships between assets. This comprehensive view allows organizations to quickly identify and address vulnerabilities affecting specific assets. References:

? CompTIA SecurityX Study Guide: Discusses the role of CMDBs in asset management and vulnerability identification.
? ITIL (Information Technology Infrastructure Library) Framework: Recommends the use of CMDBs for effective configuration and asset management.
? "Configuration Management Best Practices" by Bob Aiello and Leslie Sachs: Covers the importance of CMDBs in managing IT assets and addressing vulnerabilities.

NEW QUESTION 4

A company is having issues with its vulnerability management program New devices/IPs are added and dropped regularly, making the vulnerability report inconsistent Which of the following actions should the company lake to most likely improve the vulnerability management process'

- A. Request a weekly report with all new assets deployed and decommissioned
- B. Extend the DHCP lease lime to allow the devices to remain with the same address for a longer period.
- C. Implement a shadow IT detection process to avoid rogue devices on the network
- D. Perform regular discovery scanning throughout the 11 landscape using the vulnerability management tool

Answer: D

Explanation:

To improve the vulnerability management process in an environment where new devices/IPs are added and dropped regularly, the company should perform regular discovery scanning throughout the IT landscape using the vulnerability management tool. Here??s why:

? Accurate Asset Inventory: Regular discovery scans help maintain an up-to-date inventory of all assets, ensuring that the vulnerability management process includes all relevant devices and IPs.

? Consistency in Reporting: By continuously discovering and scanning new and existing assets, the company can generate consistent and comprehensive vulnerability reports that reflect the current state of the network.

? Proactive Management: Regular scans enable the organization to proactively identify and address vulnerabilities on new and existing assets, reducing the window of exposure to potential threats.

? References:

NEW QUESTION 5

A company detects suspicious activity associated with external connections Security detection tools are unable to categorize this activity. Which of the following is the best solution to help the company overcome this challenge?

- A. Implement an Interactive honeypot
- B. Map network traffic to known IoCs.
- C. Monitor the dark web
- D. implement UEBA

Answer: D

Explanation:

User and Entity Behavior Analytics (UEBA) is the best solution to help the company overcome challenges associated with suspicious activity that cannot be categorized by traditional detection tools. UEBA uses advanced analytics to establish baselines of normal behavior for users and entities within the network. It then identifies deviations from these baselines, which may indicate malicious activity. This approach is particularly effective for detecting unknown threats and sophisticated attacks that do not match known indicators of compromise (IoCs).

Reference: CompTIA SecurityX Study Guide, Chapter on Advanced Threat Detection and Mitigation, Section on User and Entity Behavior Analytics (UEBA).

NEW QUESTION 6

A security analyst discovered requests associated with IP addresses known for born legitimate 3nd bot-related traffic. Which of the following should the analyst use to determine whether the requests are malicious?

- A. User-agent string
- B. Byte length of the request
- C. Web application headers
- D. HTML encoding field

Answer: A

Explanation:

The user-agent string can provide valuable information to distinguish between legitimate and bot-related traffic. It contains details about the browser, device, and sometimes the operating system of the client making the request.

Why Use User-Agent String?

? Identify Patterns: User-agent strings can help identify patterns that are typical of bots or legitimate users.

? Block Malicious Bots: Many bots use known user-agent strings, and identifying these can help block malicious requests.

? Anomalies Detection: Anomalous user-agent strings can indicate spoofing attempts or malicious activity.

Other options provide useful information but may not be as effective for initial determination of the nature of the request:

? B. Byte length of the request: This can indicate anomalies but does not provide detailed information about the client.

? C. Web application headers: While useful, they may not provide enough distinction between legitimate and bot traffic.

? D. HTML encoding field: This is not typically used for identifying the nature of the request.

References:

? CompTIA SecurityX Study Guide

? "User-Agent Analysis for Security," OWASP

? NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)"

NEW QUESTION 7

A security analyst is reviewing the following log:

Time	File type	Size	Antivirus status	Location
11:25	txt	25mb	block	c:\
11:27	dll	10mb	allow	c:\temp
11:29	doc	37mb	block	c:\users\user1\Desktop
11:32	pdf	13mb	allow	c:\users\user2\Downloads
11:35	txt	49mb	allow	c:\users\user3\Documents

Which of the following possible events should the security analyst investigate further?

- A. A macro that was prevented from running
- B. A text file containing passwords that were leaked
- C. A malicious file that was run in this environment
- D. A PDF that exposed sensitive information improperly

Answer: B

Explanation:

Based on the log provided, the most concerning event that should be investigated further is the presence of a text file containing passwords that were leaked. Here's why:

? Sensitive Information Exposure: A text file containing passwords represents a significant security risk, as it indicates that sensitive credentials have been exposed in plain text, potentially leading to unauthorized access.

? Immediate Threat: Password leaks can lead to immediate exploitation by attackers, compromising user accounts and sensitive data. This requires urgent investi

NEW QUESTION 8

A global manufacturing company has an internal application mat is critical to making products This application cannot be updated and must Be available in the production area A security architect is implementing security for the application. Which of the following best describes the action the architect should take-?

- A. Disallow wireless access to the application.
- B. Deploy Intrusion detection capabilities using a network tap
- C. Create an acceptable use policy for the use of the application
- D. Create a separate network for users who need access to the application

Answer: D

Explanation:

Creating a separate network for users who need access to the application is the best action to secure an internal application that is critical to the production area and cannot be updated.

Why Separate Network?

? Network Segmentation: Isolates the critical application from the rest of the network, reducing the risk of compromise and limiting the potential impact of any security incidents.

? Controlled Access: Ensures that only authorized users have access to the application, enhancing security and reducing the attack surface.

? Minimized Risk: Segmentation helps in protecting the application from vulnerabilities that could be exploited from other parts of the network.

Other options, while beneficial, do not provide the same level of security for a critical application:

? A. Disallow wireless access: Useful but does not provide comprehensive protection.

? B. Deploy intrusion detection capabilities using a network tap: Enhances monitoring but does not provide the same level of isolation and control.

? C. Create an acceptable use policy: Important for governance but does not provide technical security controls.

References:

? CompTIA SecurityX Study Guide

? NIST Special Publication 800-125, "Guide to Security for Full Virtualization Technologies"

? "Network Segmentation Best Practices," Cisco Documentation

NEW QUESTION 9

Which of the following is the main reason quantum computing advancements are leading companies and countries to deploy new encryption algorithms?

- A. Encryption systems based on large prime numbers will be vulnerable to exploitation
- B. Zero Trust security architectures will require homomorphic encryption.
- C. Perfect forward secrecy will prevent deployment of advanced firewall monitoring techniques
- D. Quantum computers will enable malicious actors to capture IP traffic in real time

Answer: A

Explanation:

Advancements in quantum computing pose a significant threat to current encryption systems, especially those based on the difficulty of factoring large prime numbers, such as RSA. Quantum computers have the potential to solve these problems exponentially faster than classical computers, making current cryptographic systems vulnerable.

Why Large Prime Numbers are Vulnerable:

? Shor's Algorithm: Quantum computers can use Shor's algorithm to factorize large integers efficiently, which undermines the security of RSA encryption.

? Cryptographic Breakthrough: The ability to quickly factor large prime numbers means that encrypted data, which relies on the hardness of this mathematical problem, can be decrypted.

Other options, while relevant, do not capture the primary reason for the shift towards new encryption algorithms:

? B. Zero Trust security architectures: While important, the shift to homomorphic encryption is not the main driver for new encryption algorithms.

? C. Perfect forward secrecy: It enhances security but is not the main reason for new encryption algorithms.

? D. Real-time IP traffic capture: Quantum computers pose a more significant threat to the underlying cryptographic algorithms than to the real-time capture of

traffic.

References:

? CompTIA SecurityX Study Guide

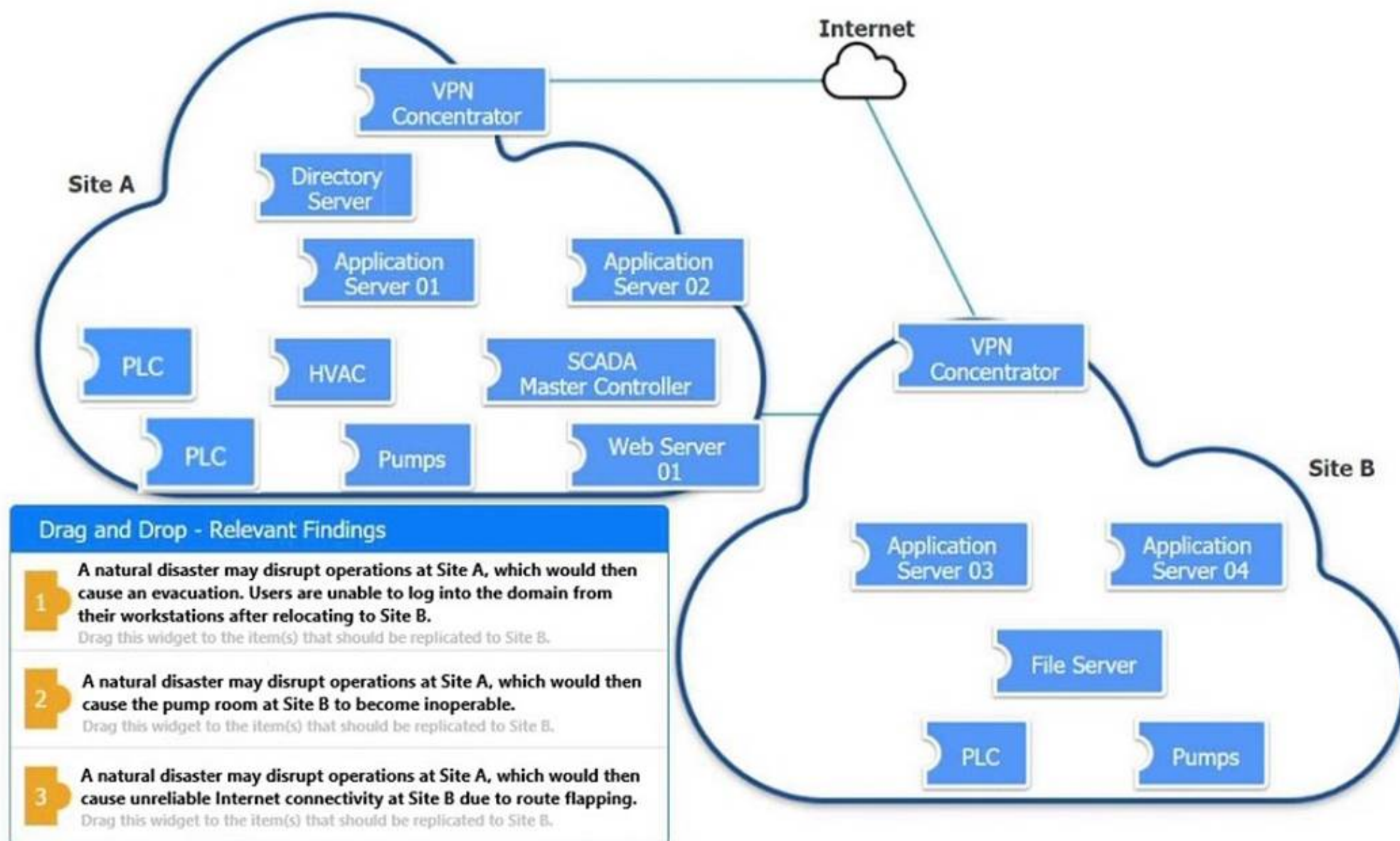
? NIST Special Publication 800-208, "Recommendation for Stateful Hash-Based Signature Schemes"

? "Quantum Computing and Cryptography," MIT Technology Review

NEW QUESTION 10

DRAG DROP

An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS

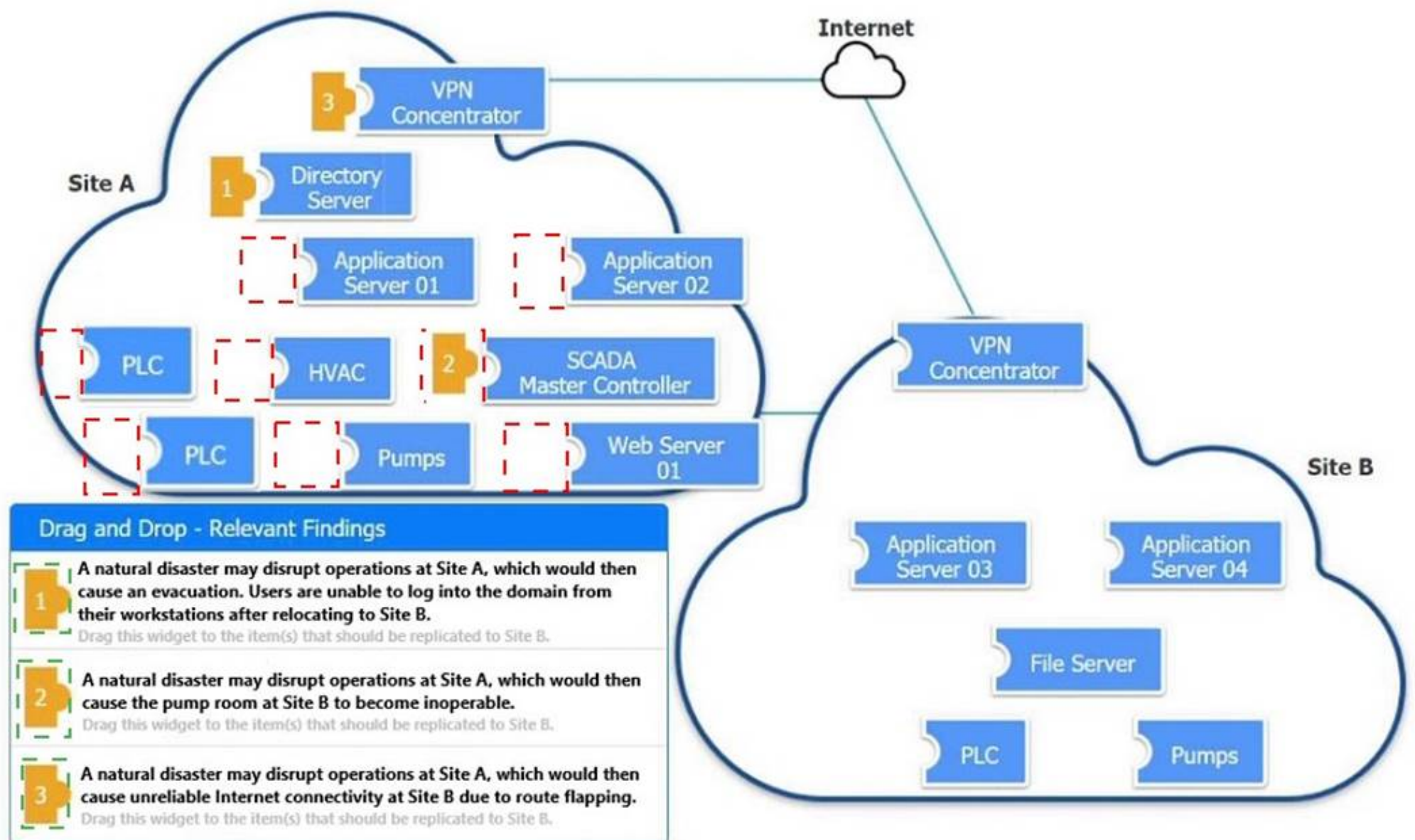


Review the following scenarios and instructions. Match each relevant finding to the affected host.

After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

Each finding may be used more than once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

✖

A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.

Corrective Action

Modify the BGP configuration
▼

NEW QUESTION 10

Developers have been creating and managing cryptographic material on their personal laptops fix use in production environment. A security engineer needs to initiate a more secure process. Which of the following is the best strategy for the engineer to use?

- A. Disabling the BIOS and moving to UEFI
- B. Managing secrets on the vTPM hardware
- C. Employing shielding to prevent LMI
- D. Managing key material on a HSM

Answer: D

Explanation:

The best strategy for securely managing cryptographic material is to use a Hardware Security Module (HSM). Here??s why:
 ? Security and Integrity: HSMs are specialized hardware devices designed to protect and manage digital keys. They provide high levels of physical and logical security, ensuring that cryptographic material is well protected against tampering and unauthorized access.
 ? Centralized Key Management: Using HSMs allows for centralized management of cryptographic keys, reducing the risks associated with decentralized and potentially insecure key storage practices, such as on personal laptops.

? Compliance and Best Practices: HSMs comply with various industry standards and regulations (such as FIPS 140-2) for secure key management. This ensures that the organization adheres to best practices and meets compliance requirements.

? References:

NEW QUESTION 14

An audit finding reveals that a legacy platform has not retained logs for more than 30 days. The platform has been segmented due to its interoperability with newer technology. As a temporary solution, the IT department changed the log retention to 120 days. Which of the following should the security engineer do to ensure the logs are being properly retained?

- A. Configure a scheduled task nightly to save the logs
- B. Configure event-based triggers to export the logs at a threshold.
- C. Configure the SIEM to aggregate the logs
- D. Configure a Python script to move the logs into a SQL database.

Answer: C

Explanation:

To ensure that logs from a legacy platform are properly retained beyond the default retention period, configuring the SIEM to aggregate the logs is the best approach. SIEM solutions are designed to collect, aggregate, and store logs from various sources, providing centralized log management and retention. This setup ensures that logs are retained according to policy and can be easily accessed for analysis and compliance purposes. References:

? CompTIA SecurityX Study Guide: Discusses the role of SIEM in log management and retention.

? NIST Special Publication 800-92, "Guide to Computer Security Log Management": Recommends the use of centralized log management solutions, such as SIEM, for effective log retention and analysis.

? "Security Information and Event Management (SIEM) Implementation" by David Miller: Covers best practices for configuring SIEM systems to aggregate and retain logs from various sources.

NEW QUESTION 19

A security engineer performed a code scan that resulted in many false positives. The security engineer must find a solution that improves the quality of scanning results before application deployment. Which of the following is the best solution?

- A. Limiting the tool to a specific coding language and tuning the rule set
- B. Configuring branch protection rules and dependency checks
- C. Using an application vulnerability scanner to identify coding flaws in production
- D. Performing updates on code libraries before code development

Answer: A

Explanation:

To improve the quality of code scanning results and reduce false positives, the best solution is to limit the tool to a specific coding language and fine-tune the rule set. By configuring the code scanning tool to focus on the specific language used in the application, the tool can more accurately identify relevant issues and reduce the number of false positives. Additionally, tuning the rule set ensures that the tool's checks are appropriate for the application's context, further improving the accuracy of the scan results.

References:

? CompTIA SecurityX Study Guide: Discusses best practices for configuring code scanning tools, including language-specific tuning and rule set adjustments.

? "Secure Coding: Principles and Practices" by Mark G. Graff and Kenneth R. van Wyk: Highlights the importance of customizing code analysis tools to reduce false positives.

? OWASP (Open Web Application Security Project): Provides guidelines for configuring and tuning code scanning tools to improve accuracy.

NEW QUESTION 23

A systems administrator wants to use existing resources to automate reporting from disparate security appliances that do not currently communicate. Which of the following is the best way to meet this objective?

- A. Configuring an API Integration to aggregate the different data sets
- B. Combining back-end application storage into a single, relational database
- C. Purchasing and deploying commercial off the shelf aggregation software
- D. Migrating application usage logs to on-premises storage

Answer: A

Explanation:

The best way to automate reporting from disparate security appliances that do not currently communicate is to configure an API Integration to aggregate the different data sets. Here's why:

? Interoperability: APIs allow different systems to communicate and share data, even

if they were not originally designed to work together. This enables the integration of various security appliances into a unified reporting system.

? Automation: API integrations can automate the process of data collection, aggregation, and reporting, reducing manual effort and increasing efficiency.

? Scalability: APIs provide a scalable solution that can easily be extended to include additional security appliances or data sources as needed.

? References:

NEW QUESTION 25

Third parties notified a company's security team about vulnerabilities in the company's application. The security team determined these vulnerabilities were previously disclosed in third-party libraries. Which of the following solutions best addresses the reported vulnerabilities?

- A. Using IaC to include the newest dependencies
- B. Creating a bug bounty program
- C. Implementing a continuous security assessment program
- D. Integrating a SAST tool as part of the pipeline

Answer: D

Explanation:

The best solution to address reported vulnerabilities in third-party libraries is integrating a Static Application Security Testing (SAST) tool as part of the development pipeline. Here's why:

- ? Early Detection: SAST tools analyze source code for vulnerabilities before the code is compiled. This allows developers to identify and fix security issues early in the development process.
- ? Continuous Security: By integrating SAST tools into the CI/CD pipeline, the organization ensures continuous security assessment of the codebase, including third-party libraries, with each code commit and build.
- ? Comprehensive Analysis: SAST tools provide a detailed analysis of the code, identifying potential vulnerabilities in both proprietary code and third-party dependencies, ensuring that known issues in libraries are addressed promptly.
- ? References:

NEW QUESTION 29

A company recently experienced an incident in which an advanced threat actor was able to shim malicious code against the hardware static of a domain controller. The forensic team cryptographically validated that the underlying firmware of the box and the operating system had not been compromised. However, the attacker was able to exfiltrate information from the server using a steganographic technique within LDAP. Which of the following is the best way to reduce the risk of reoccurrence?

- A. Enforcing allow lists for authorized network ports and protocols
- B. Measuring and attesting to the entire boot chain
- C. Rolling the cryptographic keys used for hardware security modules
- D. Using code signing to verify the source of OS updates

Answer: A

Explanation:

The scenario describes a sophisticated attack where the threat actor used steganography within LDAP to exfiltrate data. Given that the hardware and OS firmware were validated and found uncompromised, the attack vector likely exploited a network communication channel. To mitigate such risks, enforcing allow lists for authorized network ports and protocols is the most effective strategy.

Here's why this option is optimal:

- ? Port and Protocol Restrictions: By creating an allow list, the organization can restrict communications to only those ports and protocols that are necessary for legitimate business operations. This reduces the attack surface by preventing unauthorized or unusual traffic.
- ? Network Segmentation: Enforcing such rules helps in segmenting the network and ensuring that only approved communications occur, which is critical in preventing data exfiltration methods like steganography.
- ? Preventing Unauthorized Access: Allow lists ensure that only predefined, trusted connections are allowed, blocking potential paths that attackers could use to infiltrate or exfiltrate data.

Other options, while beneficial in different contexts, are not directly addressing the network communication threat:

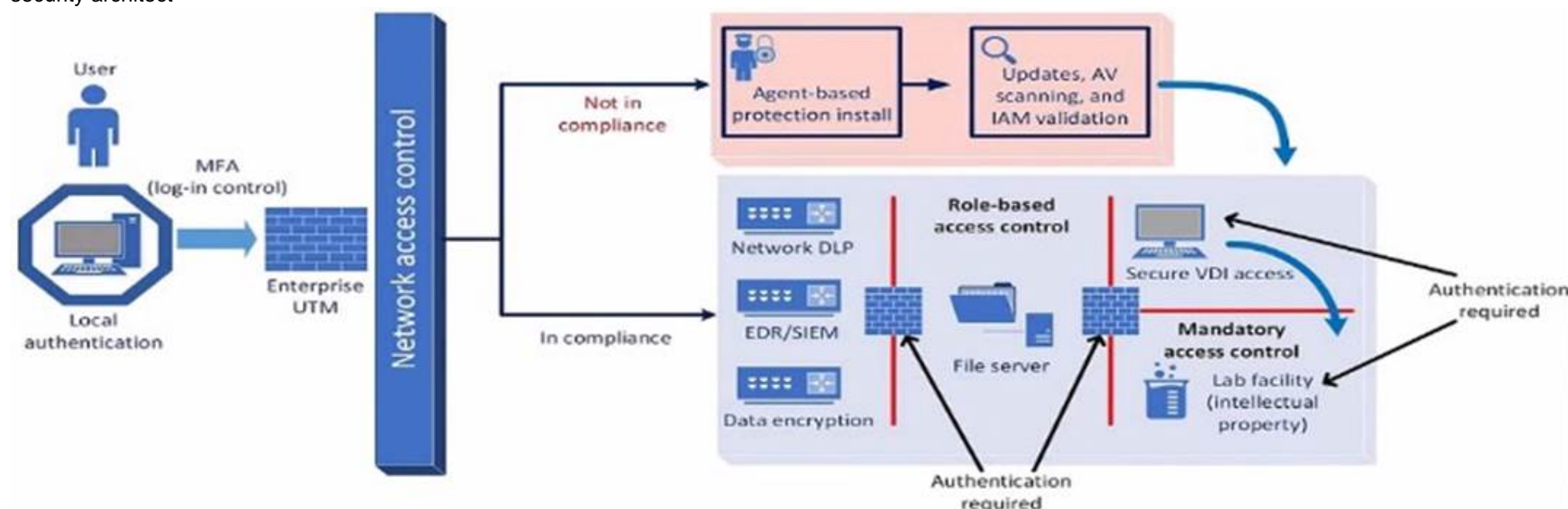
- ? B. Measuring and attesting to the entire boot chain: While this improves system integrity, it doesn't directly mitigate the risk of data exfiltration through network channels.
- ? C. Rolling the cryptographic keys used for hardware security modules: This is useful for securing data and communications but doesn't directly address the specific method of exfiltration described.
- ? D. Using code signing to verify the source of OS updates: Ensures updates are from legitimate sources, but it doesn't mitigate the risk of network-based data exfiltration.

References:

- ? CompTIA SecurityX Study Guide
- ? NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy"
- ? CIS Controls Version 8, Control 9: Limitation and Control of Network Ports, Protocols, and Services

NEW QUESTION 30

A company plans to implement a research facility with Intellectual property data that should be protected. The following is the security diagram proposed by the security architect.



Which of the following security architect models is illustrated by the diagram?

- A. Identity and access management model
- B. Agent based security model
- C. Perimeter protection security model
- D. Zero Trust security model

Answer: D

Explanation:

The security diagram proposed by the security architect depicts a Zero Trust security model. Zero Trust is a security framework that assumes all entities, both inside and outside the network, cannot be trusted and must be verified before gaining access to resources.

Key Characteristics of Zero Trust in the Diagram:

- ? Role-based Access Control: Ensures that users have access only to the resources necessary for their role.
- ? Mandatory Access Control: Additional layer of security requiring authentication for access to sensitive areas.
- ? Network Access Control: Ensures that devices meet security standards before accessing the network.
- ? Multi-factor Authentication (MFA): Enhances security by requiring multiple forms of verification.

This model aligns with the Zero Trust principles of never trusting and always verifying access requests, regardless of their origin.

References:

- ? CompTIA SecurityX Study Guide
- ? NIST Special Publication 800-207, "Zero Trust Architecture"
- ? "Implementing a Zero Trust Architecture," Forrester Research

NEW QUESTION 31

A company that relies on an COL system must keep it operating until a new solution is available Which of the following is the most secure way to meet this goal?

- A. Isolating the system and enforcing firewall rules to allow access to only required endpoints
- B. Enforcing strong credentials and improving monitoring capabilities
- C. Restricting system access to perform necessary maintenance by the IT team
- D. Placing the system in a screened subnet and blocking access from internal resources

Answer: A

Explanation:

To ensure the most secure way of keeping a legacy system (COL) operating until a new solution is available, isolating the system and enforcing strict firewall rules is the best approach. This method minimizes the attack surface by restricting access to only the necessary endpoints, thereby reducing the risk of unauthorized access and potential security breaches. Isolating the system ensures that it is not exposed to the broader network, while firewall rules control the traffic that can reach the system, providing a secure environment until a replacement is implemented.

References:

- ? CompTIA SecurityX Study Guide: Recommends network isolation and firewall rules as effective measures for securing legacy systems.
 - ? NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security": Advises on isolating critical systems and using firewalls to control access.
 - ? "Network Security Assessment" by Chris McNab: Discusses techniques for isolating systems and enforcing firewall rules to protect vulnerable or legacy systems.
- By isolating the system and implementing strict firewall controls, the organization can maintain the necessary operations securely while working on deploying a new solution.

NEW QUESTION 35

A security analyst is reviewing the following event timeline from an COR solution:

Time	File name	File action	Action verdict
4:08 p.m.	hr-reporting.docx	File save	Allowed
4:09 p.m.	hr-reporting.docx	Scan initiated	Pending
4:10 p.m.	hr-reporting.docx	File execute	Allowed
4:16 p.m.	paychecks.xlsx	File save	Allowed
4:16 p.m.	paychecks.xlsx	File shared	Allowed
4:17 p.m.	hr-reporting.docx	Script launched	Allowed
4:19 p.m.	hr-reporting.docx	Scan complete	Malware found
4:20 p.m.	paychecks.xlsx	File edit	Allowed

Which of the following most likely has occurred and needs to be fixed?

- A. The DI P has failed to block malicious exfiltration and data tagging is not being utilized property
- B. An EDR bypass was utilized by a threat actor and updates must be installed by the administrator.
- C. A logic law has introduced a TOCTOU vulnerability and must be addressed by the COR vendor
- D. A potential insider threat is being investigated and will be addressed by the senior management team.

Answer: C

Explanation:

The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed. This suggests a Time-Of- Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.

References:

- ? CompTIA SecurityX Study Guide: Discusses TOCTOU vulnerabilities as a timing attack where the state of a resource changes after it has been validated.
- ? NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations": Recommends addressing TOCTOU vulnerabilities to ensure the integrity of security operations.
- ? "The Art of Software Security Assessment" by Mark Dowd, John McDonald, and Justin Schuh: Covers logic flaws and timing vulnerabilities, including TOCTOU

issues.

NEW QUESTION 40

A security analyst is reviewing suspicious log-in activity and sees the following data in the SICM:

Account	Application	Authorization server	Status	Risk
SALES1	Customer manager	LDAP-US	Success	Low
SALES1	Payroll	LDAP-US	Success	Low
ADMIN	Email	LDAP-US	Failure	High
SALES1	Email	LDAP-EU	Unknown	Unknown
MARKET1	Customer manager	LDAP-US	Success	Low
FINANCE1	Payroll	LDAP-EU	Unknown	Unknown

Which of the following is the most appropriate action for the analyst to take?

- A. Update the log configuration settings on the directory server that is not being captured properly.
- B. Have the admin account owner change their password to avoid credential stuffing.
- C. Block employees from logging in to applications that are not part of their business area.
- D. Implement automation to disable accounts that have been associated with high-risk activity.

Answer: D

Explanation:

The log-in activity indicates a security threat, particularly involving the ADMIN account with a high-risk failure status. This suggests that the account may be targeted by malicious activities such as credential stuffing or brute force attacks.

? Updating log configuration settings (A) may help in better logging future activities but does not address the immediate threat.

? Changing the admin account password (B) is a good practice but may not fully mitigate the ongoing threat if the account has already been compromised.

? Blocking employees (C) from logging into non-business applications might help in reducing attack surfaces but doesn't directly address the compromised account issue.

Implementing automation to disable accounts associated with high-risk activities ensures an immediate response to the detected threat, preventing further unauthorized access and allowing time for thorough investigation and remediation.

References:

? CompTIA SecurityX guide on incident response and account management.

? Best practices for handling compromised accounts.

? Automation tools and techniques for security operations centers (SOCs).

NEW QUESTION 43

After an incident occurred, a team reported during the lessons-learned review that the team.

* Lost important information for further analysis.

* Did not utilize the chain of communication

* Did not follow the right steps for a proper response

Which of the following solutions is the best way to address these findings?

- A. Requesting budget for better forensic tools to improve technical capabilities for incident response operations
- B. Building playbooks for different scenarios and performing regular table-top exercises
- C. Requiring professional incident response certifications for each new team member
- D. Publishing the incident response policy and enforcing it as part of the security awareness program

Answer: B

Explanation:

Building playbooks for different scenarios and performing regular table-top exercises directly addresses the issues identified in the lessons-learned review. Here's why:

? Lost important information for further analysis: Playbooks outline step-by-step procedures for incident response, ensuring that team members know exactly what to document and how to preserve evidence.

? Did not utilize the chain of communication: Playbooks include communication protocols, specifying who to notify and when. Regular table-top exercises reinforce these communication channels, ensuring they are followed during actual incidents.

? Did not follow the right steps for a proper response: Playbooks provide a clear sequence of actions to be taken during various types of incidents, helping the team to respond in a structured and effective manner. Regular exercises allow the team to practice these steps, identifying and correcting any deviations from the plan.

Investing in better forensic tools (Option A) or requiring certifications (Option C) are also valuable, but they do not directly address the procedural and communication gaps identified. Publishing and enforcing the incident response policy (Option D) is important but not as practical and hands-on as playbooks and exercises in ensuring the team is prepared.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"

? SANS Institute, "Incident Handler's Handbook"

NEW QUESTION 45

A security architect for a global organization with a distributed workforce recently received funding to deploy a CASB solution. Which of the following most likely explains the choice to use a proxy-based CASB?

- A. The capability to block unapproved applications and services is possible.
- B. Privacy compliance obligations are bypassed when using a user-based deployment.
- C. Protecting and regularly rotating API secret keys requires a significant time commitment.
- D. Corporate devices cannot receive certificates when not connected to on-premises devices.

Answer: A

Explanation:

A proxy-based Cloud Access Security Broker (CASB) is chosen primarily for its ability to block unapproved applications and services. Here's why:

? **Application and Service Control:** Proxy-based CASBs can monitor and control the

use of applications and services by inspecting traffic as it passes through the proxy. This allows the organization to enforce policies that block unapproved applications and services, ensuring compliance with security policies.

? **Visibility and Monitoring:** By routing traffic through the proxy, the CASB can

provide detailed visibility into user activities and data flows, enabling better monitoring and threat detection.

? **Real-Time Protection:** Proxy-based CASBs can provide real-time protection

against threats by analyzing and controlling traffic before it reaches the end user, thus preventing the use of risky applications and services.

? **References:**

NEW QUESTION 50**SIMULATION**

A product development team has submitted code snippets for review prior to release. **INSTRUCTIONS**

Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.

Code Snippet 1

Code Snippet 1

Code Snippet 2

Web browser:

URL: `https://comptia.org/profiles/userdetails?userid=103`

Web server code:

--

```
String accountQuery = "SELECT * from users WHERE userid = ?";
```

```
PreparedStatement stmt = connection.prepareStatement(accountQuery);
```

```
stmt.setString(1, request.getParameter("userid"));
```

```
ResultSet queryResponse = stmt.executeQuery();
```

--

Code Snippet 2


```
Caller:
URL: https://comptia.org/api/userprofile?userid=103

API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5', 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
    userId = request.getParam(userid)

    ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                  -h loginserver.comptia.org
                  -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
    accountLookup = subprocess.Popen(ldapLookup)

    if (userExists(accountLookup))
        accountFound = true
    else
        accountFound = false
    ...
```

Vulnerability 1:

- ? SQL injection
- ? Cross-site request forgery
- ? Server-side request forgery
- ? Indirect object reference
- ? Cross-site scripting

Fix 1:

- ? Perform input sanitization of the userid field.
- ? Perform output encoding of queryResponse,
- ? Ensure usex:ia belongs to logged-in user.
- ? Inspect URLs and disallow arbitrary requests.
- ? Implement anti-forgery tokens.

Vulnerability 2

- 1) Denial of service
- 2) Command injection
- 3) SQL injection
- 4) Authorization bypass
- 5) Credentials passed via GET

Fix 2

- A) Implement prepared statements and bind variables.
- B) Remove the serve_forever instruction.
- C) Prevent the "authenticated" value from being overridden by a GET parameter.
- D) HTTP POST should be used for sensitive parameters.
- E) Perform input sanitization of the userid field.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Code Snippet 1

Vulnerability 1: SQL injection

SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.

Fix 1: Perform input sanitization of the userid field.

Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.

Code Snippet 2

Vulnerability 2: Cross-site request forgery

Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.

Fix 2: Implement anti-forgery tokens.

Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

NEW QUESTION 55

A senior security engineer flags me following log file snippet as having likely facilitated an attacker's lateral movement in a recent breach:

```
[log.txt]
...
qry_source: 19.27.214.22 TCP/53
qry_dest: 199.105.22.13 TCP/53
qry_type: AXFR
| in ccmptia.org
-----| directoryserver1 A 10.80.8.10
-----| directoryserver2 A 10.80.8.11
-----| directoryserver3 A 10.80.8.12
-----| internal-dns A 10.80.9.1
-----| www-int A 10.80.9.3
-----| fshare A 10.80.9.4
-----| sip A 10.80.9.5
-----| man-crit-apps A 10.81.22.33
...
```

Which of the following solutions, if implemented, would mitigate the risk of this issue reoccurring?

- A. Disabling DNS zone transfers
- B. Restricting DNS traffic to UDP/W
- C. Implementing DNS masking on internal servers
- D. Permitting only clients from internal networks to query DNS

Answer: A

Explanation:

The log snippet indicates a DNS AXFR (zone transfer) request, which can be exploited by attackers to gather detailed information about an internal network's infrastructure. Disabling DNS zone transfers is the best solution to mitigate this risk. Zone transfers should generally be restricted to authorized secondary DNS servers and not be publicly accessible, as they can reveal sensitive network information that facilitates lateral movement during an attack.

References:

? CompTIA SecurityX Study Guide: Discusses the importance of securing DNS configurations, including restricting zone transfers.

? NIST Special Publication 800-81, "Secure Domain Name System (DNS) Deployment Guide": Recommends restricting or disabling DNS zone transfers to prevent information leakage.

NEW QUESTION 60

A security engineer needs to secure the OT environment based on the following requirements

- Isolate the OT network segment
- Restrict Internet access.
- Apply security updates to workstations
- Provide remote access to third-party vendors

Which of the following design strategies should the engineer implement to best meet these requirements?

- A. Deploy a jump box on the third party network to access the OT environment and provide updates using a physical delivery method on the workstations
- B. Implement a bastion host in the OT network with security tools in place to monitor access and use a dedicated update server for the workstations.
- C. Enable outbound internet access on the OT firewall to any destination IP address and use the centralized update server for the workstations
- D. Create a staging environment on the OT network for the third-party vendor to access and enable automatic updates on the workstations.

Answer: B

Explanation:

To secure the Operational Technology (OT) environment based on the given requirements, the best approach is to implement a bastion host in the OT network. The bastion host serves as a secure entry point for remote access, allowing third-party vendors to connect while being monitored by security tools. Using a dedicated update server for workstations ensures that security updates are applied in a controlled manner without direct internet access.

References:

? CompTIA SecurityX Study Guide: Recommends the use of bastion hosts and dedicated update servers for securing OT environments.

? NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security": Advises on isolating OT networks and using secure remote access methods.

? "Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill: Discusses strategies for securing OT networks, including the use of bastion hosts and update servers.

NEW QUESTION 63

A systems engineer is configuring a system baseline for servers that will provide email services. As part of the architecture design, the engineer needs to improve performance of the systems by using an access vector cache, facilitating mandatory access control and protecting against:

- Unauthorized reading and modification of data and programs
- Bypassing application security mechanisms
- Privilege escalation
- interference with other processes

Which of the following is the most appropriate for the engineer to deploy?

- A. SELinux
- B. Privileged access management
- C. Self-encrypting disks
- D. NIPS

Answer: A

Explanation:

The most appropriate solution for the systems engineer to deploy is SELinux (Security- Enhanced Linux). Here's why:

? Mandatory Access Control (MAC): SELinux enforces MAC policies, ensuring that

only authorized users and processes can access specific resources. This helps in preventing unauthorized reading and modification of data and programs.

? Access Vector Cache: SELinux utilizes an access vector cache (AVC) to improve

performance. The AVC caches access decisions, reducing the need for repetitive policy lookups and thus improving system efficiency.

? Security Mechanisms: SELinux provides a robust framework to enforce security

policies and prevent bypassing of application security mechanisms. It controls access based on defined policies, ensuring that security measures are consistently applied.

? Privilege Escalation and Process Interference: SELinux limits the ability of

processes to escalate privileges and interfere with each other by enforcing strict access controls. This containment helps in isolating processes and minimizing the risk of privilege escalation attacks.

? References:

NEW QUESTION 64

A software company deployed a new application based on its internal code repository Several customers are reporting anti-malware alerts on workstations used to test the application Which of the following is the most likely cause of the alerts?

- A. Misconfigured code commit
- B. Unsecure bundled libraries
- C. Invalid code signing certificate
- D. Data leakage

Answer: B

Explanation:

The most likely cause of the anti-malware alerts on customer workstations is unsecure bundled libraries. When developing and deploying new applications, it is common for developers to use third-party libraries. If these libraries are not properly vetted for security, they can introduce vulnerabilities or malicious code.

Why Unsecure Bundled Libraries?

? Third-Party Risks: Using libraries that are not secure can lead to malware infections if the libraries contain malicious code or vulnerabilities.

? Code Dependencies: Libraries may have dependencies that are not secure, leading to potential security risks.

? Common Issue: This is a frequent issue in software development where libraries are used for convenience but not properly vetted for security.

Other options, while relevant, are less likely to cause widespread anti-malware alerts:

? A. Misconfigured code commit: Could lead to issues but less likely to trigger anti- malware alerts.

? C. Invalid code signing certificate: Would lead to trust issues but not typically anti- malware alerts.

? D. Data leakage: Relevant for privacy concerns but not directly related to anti- malware alerts.

References:

? CompTIA SecurityX Study Guide

? "Securing Open Source Libraries," OWASP

? "Managing Third-Party Software Security Risks," Gartner Research

NEW QUESTION 65

A company lined an email service provider called my-email.com to deliver company emails. The company stalled having several issues during the migration. A security engineer is troubleshooting and observes the following configuration snippet:

@	MX	10	email.company.com	45000
www	IN	CNAME	web01.company.com.	
email	IN	CNAME	srv01.company.com	
srv01	IN	A	192.168.1.10	
web01	IN	A	192.168.1.11	
@	IN	TXT	"v=dmARC include:company.com ~all"	

Which of the following should the security engineer modify to fix the issue? (Select two).

- A. The email CNAME record must be changed to a type A record pointing to 192.168.111
- B. The TXT record must be Changed to "v=dmARC ip4:192.168.1.10 include:my-email.com - all"
- C. The srv01 A record must be changed to a type CNAME record pointing to the email server
- D. The email CNAME record must be changed to a type A record pointing to 192.168.1.10
- E. The TXT record must be changed to "v=dkim ip4:192.168.1.11 include my-email.com - ell"
- F. The TXT record must be Changed to "v=dkim ip4:192.168.1.10 include:email-all"
- G. The srv01 A record must be changed to a type CNAME record pointing to the web01 server

Answer: BD

Explanation:

The security engineer should modify the following to fix the email migration issues:

? Email CNAME Record: The email CNAME record must be changed to a type A record pointing to 192.168.1.10. This is because CNAME records should not be used where an IP address (A record) is required. Changing it to an A record ensures direct pointing to the correct IP.

? TXT Record for DMARC: The TXT record must be changed to "v=dmARC ip4:192.168.1.10 include com -all". This ensures proper configuration of DMARC (Domain-based Message Authentication, Reporting & Conformance) to include the correct IP address and the email service provider domain.

? uk.co.certification.simulator.questionpool.PList@488ba0cc

? References:

NEW QUESTION 67

A security architect is establishing requirements to design resilience in an enterprise system that will be extended to other physical locations. The system must

- Be survivable to one environmental catastrophe
- Be recoverable within 24 hours of critical loss of availability
- Be resilient to active exploitation of one site-to-site VPN solution

- A. Load-balance connection attempts and data Ingress at internet gateways
- B. Allocate fully redundant and geographically distributed standby sites.
- C. Employ layering of routers from diverse vendors
- D. Lease space to establish cold sites throughout other countries
- E. Use orchestration to procure, provision, and transfer application workloads to cloudservices
- F. Implement full weekly backups to be stored off-site for each of the company's sites

Answer: B

Explanation:

To design resilience in an enterprise system that can survive environmental catastrophes, recover within 24 hours, and be resilient to active exploitation, the best strategy is to allocate fully redundant and geographically distributed standby sites. Here's why:

? Geographical Redundancy: Having geographically distributed standby sites ensures that if one site is affected by an environmental catastrophe, the other sites can take over, providing continuity of operations.

? Full Redundancy: Fully redundant sites mean that all critical systems and data are replicated, enabling quick recovery in the event of a critical loss of availability.

? Resilience to Exploitation: Distributing resources across multiple sites reduces the risk of a single point of failure and increases resilience against targeted attacks.

? References:

NEW QUESTION 70

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CAS-005 Exam with Our Prep Materials Via below:

<https://www.certleader.com/CAS-005-dumps.html>