

CompTIA

Exam Questions CAS-005

CompTIA SecurityX Exam



NEW QUESTION 1

A company wants to implement hardware security key authentication for accessing sensitive information systems. The goal is to prevent unauthorized users from gaining access with a stolen password. Which of the following models should the company implement to best solve this issue?

- A. Rule based
- B. Time-based
- C. Role based
- D. Context-based

Answer: D

Explanation:

Context-based authentication enhances traditional security methods by incorporating additional layers of information about the user's current environment and behavior. This can include factors such as the user's location, the time of access, the device used, and the behavior patterns. It is particularly useful in preventing unauthorized access even if an attacker has obtained a valid password.

? Rule-based (A) focuses on predefined rules and is less flexible in adapting to dynamic threats.

? Time-based (B) authentication considers the time factor but doesn't provide comprehensive protection against stolen credentials.

? Role-based (C) is more about access control based on the user's role within the organization rather than authenticating the user based on current context.

By implementing context-based authentication, the company can ensure that even if a password is compromised, the additional contextual factors required for access (which an attacker is unlikely to possess) provide a robust defense mechanism.

References:

? CompTIA SecurityX guide on authentication models and best practices.

? NIST guidelines on authentication and identity proofing.

? Analysis of multi-factor and adaptive authentication techniques.

NEW QUESTION 2

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 3

After some employees were caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation. Which of the following would the company most likely do to decrease this type of risk?

- A. Improve firewall rules to avoid access to those platforms.
- B. Implement a cloud-access security broker
- C. Create SIEM rules to raise alerts for access to those platforms
- D. Deploy an internet proxy that filters certain domains

Answer: B

Explanation:

A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and cloud service providers to combine

and interject enterprise security policies as cloud-based resources are accessed. Implementing a CASB provides several benefits:

? A. Improve firewall rules to avoid access to those platforms: This can help but is not as effective or comprehensive as a CASB.

? B. Implement a cloud-access security broker: A CASB can provide visibility into cloud application usage, enforce data security policies, and protect against data leaks by monitoring and controlling access to cloud services. It also provides advanced features like data encryption, data loss prevention (DLP), and compliance monitoring.

? C. Create SIEM rules to raise alerts for access to those platforms: This helps in monitoring but does not prevent data leaks.

? D. Deploy an internet proxy that filters certain domains: This can block access to specific sites but lacks the granular control and visibility provided by a CASB.

Implementing a CASB is the most comprehensive solution to decrease the risk of data leaks by providing visibility, control, and enforcement of security policies for cloud services. References:

? CompTIA Security+ Study Guide

? Gartner, "Magic Quadrant for Cloud Access Security Brokers"

? NIST SP 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"

NEW QUESTION 4

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 5

A news organization wants to implement workflows that allow users to request that untruthful data be retraced and scrubbed from online publications to comply with the right to be forgotten Which of the following regulations is the organization most likely trying to address'

A. GDPR

B. COPPA

C. CCPA

D. DORA

Answer: A

Explanation:

The General Data Protection Regulation (GDPR) is the regulation most likely being addressed by the news organization. GDPR includes provisions for the "right to be forgotten," which allows individuals to request the deletion of personal data that is no longer necessary for the purposes for which it was collected. This regulation aims to protect the privacy and personal data of individuals within the European Union.

References:

? CompTIA SecurityX Study Guide: Covers GDPR and its requirements, including the right to be forgotten.

? GDPR official documentation: Details the rights of individuals, including data erasure and the right to be forgotten.

? "GDPR: A Practical Guide to the General Data Protection Regulation" by IT Governance Privacy Team: Provides a comprehensive overview of GDPR compliance, including workflows for data deletion requests.

NEW QUESTION 6

Users are willing passwords on paper because of the number of passwords needed in an environment. Which of the following solutions is the best way to manage this situation and decrease risks?

A. Increasing password complexity to require 31 least 16 characters

B. implementing an SSO solution and integrating with applications

C. Requiring users to use an open-source password manager

D. Implementing an MFA solution to avoid reliance only on passwords

Answer: B

Explanation:

Implementing a Single Sign-On (SSO) solution and integrating it with applications is the best way to manage the situation and decrease risks. Here??s why:

? Reduced Password Fatigue: SSO allows users to log in once and gain access to multiple applications and systems without needing to remember and manage multiple passwords. This reduces the likelihood of users writing down passwords.

? Improved Security: By reducing the number of passwords users need to manage, SSO decreases the attack surface and potential for password-related security breaches. It also allows for the implementation of stronger authentication methods.

? User Convenience: SSO improves the user experience by simplifying the login process, which can lead to higher productivity and satisfaction.

? References:

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 that 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

A security officer received several complaints from users about excessive MFA push notifications at night. The security team investigates and suspects malicious activities regarding user account authentication. Which of the following is the best way for the security officer to restrict MFA notifications?

- A. Provisioning FIDO2 devices
- B. Deploying a text message based on MFA
- C. Enabling OTP via email
- D. Configuring prompt-driven MFA

Answer: D

Explanation:

Excessive MFA push notifications can be a sign of an attempted push notification attack, where attackers repeatedly send MFA prompts hoping the user will eventually approve one by mistake. To mitigate this:

? A. Provisioning FIDO2 devices: While FIDO2 devices offer strong authentication, they may not be practical for all users and do not directly address the issue of excessive push notifications.

? B. Deploying a text message-based MFA: SMS-based MFA can still be vulnerable to similar spamming attacks and phishing.

? C. Enabling OTP via email: Email-based OTPs add another layer of security but do not directly solve the issue of excessive notifications.

? D. Configuring prompt-driven MFA: This option allows users to respond to prompts in a secure manner, often including features like time-limited approval windows, additional verification steps, or requiring specific actions to approve. This can help prevent users from accidentally approving malicious attempts.

Configuring prompt-driven MFA is the best solution to restrict unnecessary MFA notifications and improve security.

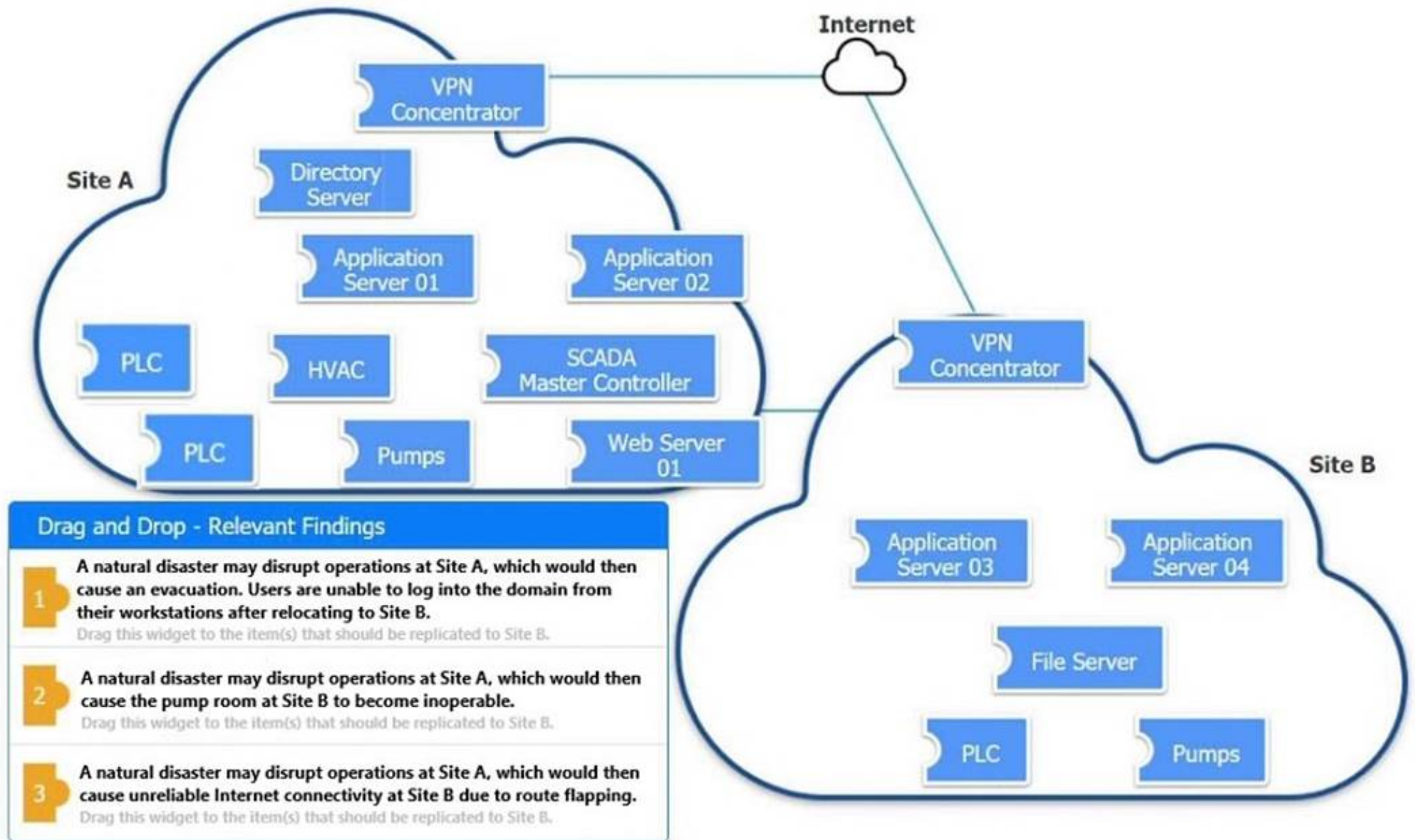
References:

? CompTIA Security+ Study Guide
 ? NIST SP 800-63B, "Digital Identity Guidelines"
 ? "Multi-Factor Authentication: Best Practices" by Microsoft

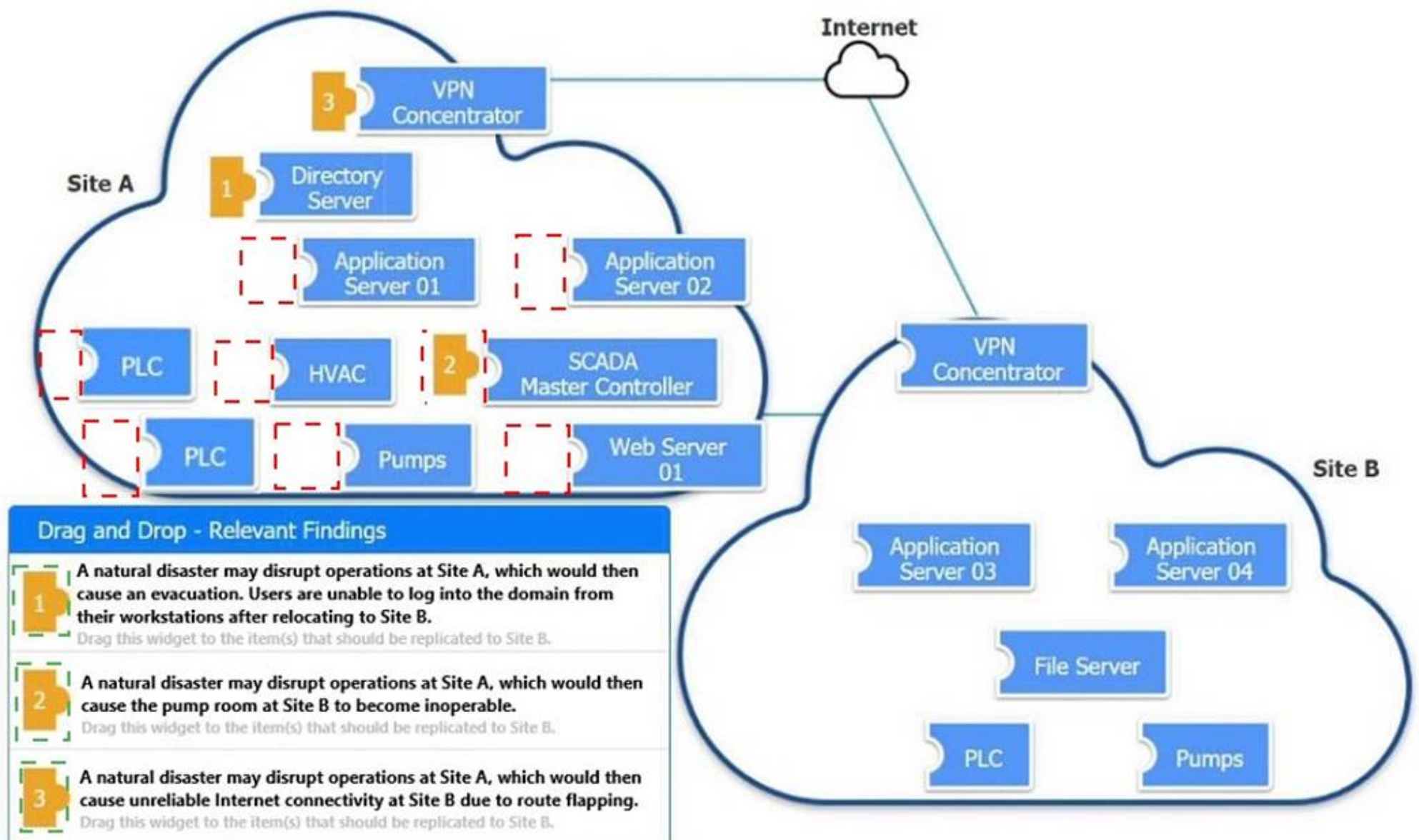
NEW QUESTION 10

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

A security analyst received a notification from a cloud service provider regarding an attack detected on a web server. The cloud service provider shared the following information about the attack:

- The attack came from inside the network.
- The attacking source IP was from the internal vulnerability scanners.
- The scanner is not configured to target the cloud servers.

Which of the following actions should the security analyst take first?

- A. Create an allow list for the vulnerability scanner IPs in order to avoid false positives
- B. Configure the scan policy to avoid targeting an out-of-scope host
- C. Set network behavior analysis rules
- D. Quarantine the scanner sensor to perform a forensic analysis

Answer: D

Explanation:

When a security analyst receives a notification about an attack that appears to originate from an internal vulnerability scanner, it suggests that the scanner itself might have been compromised. This situation is critical because a compromised scanner can potentially conduct unauthorized scans, leak sensitive information, or execute malicious actions within the network. The appropriate first action involves containing the threat to prevent further damage and allow for a thorough investigation.

Here's why quarantining the scanner sensor is the best immediate action:

• **Containment and Isolation:** Quarantining the scanner will immediately prevent it

from continuing any malicious activity or scans. This containment is crucial to protect the rest of the network from potential harm.

• **Forensic Analysis:** By isolating the scanner, a forensic analysis can be performed to understand how it was compromised, what actions it took, and what data or systems might have been affected. This analysis will provide valuable insights into the nature of the attack and help in taking appropriate remedial actions.

• **Preventing Further Attacks:** If the scanner is allowed to continue operating, it might execute more unauthorized actions, leading to greater damage. Quarantine ensures that the threat is neutralized promptly.

• **Root Cause Identification:** A forensic analysis can help identify vulnerabilities in the scanner's configuration, software, or underlying system that allowed the compromise. This information is essential for preventing future incidents.

Other options, while potentially useful in the long term, are not appropriate as immediate actions in this scenario:

• **A. Create an allow list for the vulnerability scanner IPs to avoid false positives:**

This action addresses false positives but does not mitigate the immediate threat posed by the compromised scanner.

• **B. Configure the scan policy to avoid targeting an out-of-scope host:** This step is preventive for future scans but does not deal with the current incident where the scanner is already compromised.

• **C. Set network behavior analysis rules:** While useful for ongoing monitoring and detection, this does not address the immediate need to stop the compromised scanner's activities.

In conclusion, the first and most crucial action is to quarantine the scanner sensor to halt any malicious activity and perform a forensic analysis to understand the scope and nature of the compromise. This step ensures that the threat is contained and provides a basis for further remediation efforts.

References:

• CompTIA SecurityX Study Guide

• NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"

NEW QUESTION 15

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 19

A company receives several complaints from customers regarding its website. An engineer implements a parser for the web server logs that generates the following output:

Browser	User location	Load time	HTTP response
Mozilla 5.0	United States	190ms	302
Chrome 110	France	1.2s	302
Microsoft Edge	India	3.7s	307
Microsoft Edge	Australia	6.4s	200

which of the following should the company implement to best resolve the issue?

- A. IDS
- B. CDN
- C. WAF
- D. NAC

Answer: B

Explanation:

The table indicates varying load times for users accessing the website from different geographic locations. Customers from Australia and India are experiencing significantly higher load times compared to those from the United States. This suggests that latency and geographical distance are affecting the website's performance.

? A. IDS (Intrusion Detection System): While an IDS is useful for detecting malicious activities, it does not address performance issues related to latency and geographical distribution of content.

? B. CDN (Content Delivery Network): A CDN stores copies of the website's content in multiple geographic locations. By serving content from the nearest server to the user, a CDN can significantly reduce load times and improve user experience globally.

? C. WAF (Web Application Firewall): A WAF protects web applications by filtering and monitoring HTTP traffic but does not improve performance related to geographical latency.

? D. NAC (Network Access Control): NAC solutions control access to network resources but are not designed to address web performance issues.

Implementing a CDN is the best solution to resolve the performance issues observed in the log output.

References:

? CompTIA Security+ Study Guide

? "CDN: Content Delivery Networks Explained" by Akamai Technologies

? NIST SP 800-44, "Guidelines on Securing Public Web Servers"

NEW QUESTION 21

Which of the following AI concerns is most adequately addressed by input sanitation?

- A. Model inversion
- B. Prompt Injection
- C. Data poisoning
- D. Non-explainable model

Answer: B

Explanation:

Input sanitation is a critical process in cybersecurity that involves validating and cleaning data provided by users to prevent malicious inputs from causing harm. In the context of AI concerns:

? A. Model inversion involves an attacker inferring sensitive data from model outputs, typically requiring sophisticated methods beyond just manipulating input data.

? B. Prompt Injection is a form of attack where an adversary provides malicious input to manipulate the behavior of AI models, particularly those dealing with natural language processing (NLP). Input sanitation directly addresses this by ensuring that inputs are cleaned and validated to remove potentially harmful commands or instructions that could alter the AI's behavior.

? C. Data poisoning involves injecting malicious data into the training set to compromise the model. While input sanitation can help by filtering out bad data, data poisoning is typically addressed through robust data validation and monitoring during the model training phase, rather than real-time input sanitation.

? D. Non-explainable model refers to the lack of transparency in how AI models make decisions. This concern is not addressed by input sanitation, as it relates more to model design and interpretability techniques.

Input sanitation is most relevant and effective for preventing Prompt Injection attacks, where the integrity of user inputs directly impacts the performance and security of AI models.

References:

- ? CompTIA Security+ Study Guide
- ? "Security of Machine Learning" by Battista Biggio, Blaine Nelson, and Pavel Laskov
- ? OWASP (Open Web Application Security Project) guidelines on input validation and injection attacks
- Top of Form Bottom of Form

NEW QUESTION 22

Company A and Company D ate merging Company A's compliance reports indicate branch protections are not in place A security analyst needs to ensure that potential threats to the software development life cycle are addressed. Which of the following should me analyst cons<der when completing this basic?

- A. If developers are unable to promote to production
- B. If DAST code is being stored to a single code repository
- C. If DAST scans are routinely scheduled
- D. If role-based training is deployed

Answer: C

Explanation:

Dynamic Application Security Testing (DAST) is crucial for identifying and addressing security vulnerabilities during the software development life cycle (SDLC). Ensuring that DAST scans are routinely scheduled helps in maintaining a secure development process. Why Routine DAST Scans?

- ? Continuous Security Assessment: Regular DAST scans help in identifying vulnerabilities in real-time, ensuring they are addressed promptly.
 - ? Compliance: Routine scans ensure that the development process complies with security standards and regulations.
 - ? Proactive Threat Mitigation: Regular scans help in early detection and mitigation of potential security threats, reducing the risk of breaches.
 - ? Integration into SDLC: Ensures security is embedded within the development process, promoting a security-first approach.
- Other options, while relevant, do not directly address the continuous assessment and proactive identification of threats:
- ? A. If developers are unable to promote to production: This is more of an operational issue than a security assessment.
 - ? B. If DAST code is being stored to a single code repository: This concerns code management rather than security testing frequency.
 - ? D. If role-based training is deployed: While important, training alone does not ensure continuous security assessment.

References:

- ? CompTIA SecurityX Study Guide
- ? OWASP Testing Guide
- ? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations"

NEW QUESTION 25

A compliance officer is reviewing the data sovereignty laws in several countries where the organization has no presence Which of the following is the most likely reason for reviewing these laws?

- A. The organization is performing due diligence of potential tax issues.
- B. The organization has been subject to legal proceedings in countries where it has a presence.
- C. The organization is concerned with new regulatory enforcement in other countries
- D. The organization has suffered brand reputation damage from incorrect media coverage

Answer: C

Explanation:

Reviewing data sovereignty laws in countries where the organization has no presence is likely due to concerns about regulatory enforcement. Data sovereignty laws dictate how data can be stored, processed, and transferred across borders. Understanding these laws is crucial for compliance, especially if the organization handles data that may be subject to foreign regulations.

- ? A. The organization is performing due diligence of potential tax issues: This is less likely as tax issues are generally not directly related to data sovereignty laws.
- ? B. The organization has been subject to legal proceedings in countries where it has a presence: While possible, this does not explain the focus on countries where the organization has no presence.
- ? C. The organization is concerned with new regulatory enforcement in other countries: This is the most likely reason. New regulations could impact the organization??s operations, especially if they involve data transfers or processing data from these countries.
- ? D. The organization has suffered brand reputation damage from incorrect media coverage: This is less relevant to the need for reviewing data sovereignty laws.

References:

- ? CompTIA Security+ Study Guide
- ? GDPR and other global data protection regulations
- ? "Data Sovereignty: The Future of Data Protection?" by Mark Burdon

NEW QUESTION 29

A security analyst reviews the following report:

	Location	Chassis manufacturer	OS	Application developer	Vendor
Product A	United States	Local company A	Debian 11	Unknown	Charlie Security Consulting
Product B	United States	Global company B	Red Hat Enterprise Linux	Developer B	BigBox Vulnerabilities

Which of the following assessments is the analyst performing?

- A. System
- B. Supply chain
- C. Quantitative
- D. Organizational

Answer: B

Explanation:

The table shows detailed information about products, including location, chassis manufacturer, OS, application developer, and vendor. This type of information is typically assessed in a supply chain assessment to evaluate the security and reliability of components and services from different suppliers.

Why Supply Chain Assessment?

? Component Evaluation: Assessing the origin and security of each component used in the products, including hardware, software, and third-party services.

? Vendor Reliability: Evaluating the security practices and reliability of vendors involved in providing components or services.

? Risk Management: Identifying potential risks associated with the supply chain, such as vulnerabilities in third-party components or insecure development practices.

Other types of assessments do not align with the detailed supplier and component information provided:

? A. System: Focuses on individual system security, not the broader supply chain.

? C. Quantitative: Focuses on numerical risk assessments, not supplier information.

? D. Organizational: Focuses on internal organizational practices, not external suppliers.

References:

? CompTIA SecurityX Study Guide

? NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"

? "Supply Chain Security Best Practices," Gartner Research

NEW QUESTION 32

A company wants to invest in research capabilities with the goal to operationalize the research output. Which of the following is the best option for a security architect to recommend?

- A. Dark web monitoring
- B. Threat intelligence platform
- C. Honeypots
- D. Continuous adversary emulation

Answer: B

Explanation:

Investing in a threat intelligence platform is the best option for a company looking to operationalize research output. A threat intelligence platform helps in collecting, processing, and analyzing threat data to provide actionable insights. These platforms integrate data from various sources, including dark web monitoring, honeypots, and other security tools, to offer a comprehensive view of the threat landscape.

Why a Threat Intelligence Platform?

? Data Integration: It consolidates data from multiple sources, including dark web monitoring and honeypots, making it easier to analyze and derive actionable insights.

? Actionable Insights: Provides real-time alerts and reports on potential threats, helping the organization take proactive measures.

? Operational Efficiency: Streamlines the process of threat detection and response, allowing the security team to focus on critical issues.

? Research and Development: Facilitates the operationalization of research output by providing a platform for continuous monitoring and analysis of emerging threats.

Other options, while valuable, do not offer the same level of integration and operationalization capabilities:

? A. Dark web monitoring: Useful for specific threat intelligence but lacks comprehensive operationalization.

? C. Honeypots: Effective for detecting and analyzing specific attack vectors but not for broader threat intelligence.

? D. Continuous adversary emulation: Important for testing defenses but not for integrating and operationalizing threat intelligence.

References:

? CompTIA SecurityX Study Guide

? "Threat Intelligence Platforms," Gartner Research

? NIST Special Publication 800-150, "Guide to Cyber Threat Information Sharing"

NEW QUESTION 37

A company wants to install a three-tier approach to separate the web, database, and application servers. A security administrator must harden the environment. Which of the following is the best solution?

- A. Deploying a VPN to prevent remote locations from accessing server VLANs
- B. Configuring a SASb solution to restrict users to server communication
- C. Implementing microsegmentation on the server VLANs
- D. Installing a firewall and making it the network core

Answer: C

Explanation:

The best solution to harden a three-tier environment (web, database, and application servers) is to implement microsegmentation on the server VLANs. Here's why:

? Enhanced Security: Microsegmentation creates granular security zones within the data center, allowing for more precise control over east-west traffic between servers. This helps prevent lateral movement by attackers who may gain access to one part of the network.

? Isolation of Tiers: By segmenting the web, database, and application servers, the organization can apply specific security policies and controls to each segment, reducing the risk of cross-tier attacks.

? Compliance and Best Practices: Microsegmentation aligns with best practices for network security and helps meet compliance requirements by ensuring that sensitive data and systems are properly isolated and protected.

? References:

? NIST Special Publication 800-150, "Guide to Cyber Threat Information Sharing"

? CompTIA SecurityX Study Guide

NEW QUESTION 41

A financial services organization is using AI to fully automate the process of deciding client loan rates. Which of the following should the organization be most concerned about from a privacy perspective?

- A. Model explainability
- B. Credential Theft
- C. Possible prompt injections
- D. Exposure to social engineering

Answer: A

Explanation:

When using AI to fully automate the process of deciding client loan rates, the primary concern from a privacy perspective is model explainability.

Why Model Explainability is Critical:

? Transparency: It ensures that the decision-making process of the AI model can be understood and explained to stakeholders, including clients.

? Accountability: Helps in identifying biases and errors in the model, ensuring that the AI is making fair and unbiased decisions.

? Regulatory Compliance: Various regulations require that decisions, especially those affecting individuals' financial status, can be explained and justified.

? Trust: Builds trust among users and stakeholders by demonstrating that the AI decisions are transparent and justifiable.

Other options, such as credential theft, prompt injections, and social engineering, are significant concerns but do not directly address the privacy and fairness implications of automated decision-making.

References:

? CompTIA SecurityX Study Guide

? "The Importance of Explainability in AI," IEEE Xplore

? GDPR Article 22, "Automated Individual Decision-Making, Including Profiling"

NEW QUESTION 45

A vulnerability can on a web server identified the following:

```
* TLS 1.2 Cipher Suites:
The server accepted the following 4 cipher suites:
TLS_RSA_WITH_DES_CBC_SHA          56
TLS_RSA_WITH_AES_128_CBC_SHA      128
TLS_RSA_WITH_3DES_EDE_CBC_SHA     168
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA 168 DH (1024 bits)
```

Which of the following actions would most likely eliminate on path decryption attacks? (Select two).

- A. Disallowing cipher suites that use ephemeral modes of operation for key agreement
- B. Removing support for CBC-based key exchange and signing algorithms
- C. Adding TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256
- D. Implementing HIPS rules to identify and block BEAST attack attempts
- E. Restricting cipher suites to only allow TLS_RSA_WITH_AES_128_CBC_SHA
- F. Increasing the key length to 256 for TLS_RSA_WITH_AES_128_CBC_SHA

Answer: BC

Explanation:

On-path decryption attacks, such as BEAST (Browser Exploit Against SSL/TLS) and other related vulnerabilities, often exploit weaknesses in the implementation of CBC (Cipher Block Chaining) mode. To mitigate these attacks, the following actions are recommended:

? B. Removing support for CBC-based key exchange and signing algorithms: CBC

mode is vulnerable to certain attacks like BEAST. By removing support for CBC-based ciphers, you can eliminate one of the primary vectors for these attacks.

Instead, use modern cipher modes like GCM (Galois/Counter Mode) which offer better security properties.

? C. Adding TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256: This cipher

suite uses Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for key exchange, which provides perfect forward secrecy. It also uses AES in GCM mode, which is not susceptible to the same attacks as CBC. SHA-256 is a strong hash function that ensures data integrity.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-52 Rev. 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"

? OWASP (Open Web Application Security Project) guidelines on cryptography and secure communication

NEW QUESTION 48

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 52

A security professional is investigating a trend in vulnerability findings for newly deployed cloud systems Given the following output:

Date	IP address	System name	Finding	Criticality rating
10/13/2023	10.123.34.98	System1	OpenSSL version 1.01	Medium
10/13/2023	10.3.114.72	System6	OpenSSL version 1.01	Medium
10/13/2023	10.12.134.45	System12	Java 11 runtime environment found	Medium
10/13/2023	10.68.65.11	System36	OpenSSL version 1.01	Medium
10/13/2023	10.23.74.9	System37	Java 11 runtime environment found	Medium
10/13/2023	10.13.124.3	System45	OpenSSL version 1.01	Medium

Which of the following actions would address the root cause of this issue?

- A. Automating the patching system to update base Images
- B. Recompiling the affected programs with the most current patches
- C. Disabling unused/unneeded ports on all servers
- D. Deploying a WAF with virtual patching upstream of the affected systems

Answer: A

Explanation:

The output shows that multiple systems have outdated or vulnerable software versions (OpenSSL 1.01 and Java 11 runtime). This suggests that the systems are not being patched regularly or effectively.

? A. Automating the patching system to update base images: Automating the patching process ensures that the latest security updates and patches are applied to all systems, including newly deployed ones. This addresses the root cause by ensuring that base images used for deployment are always up-to-date with the latest security patches.

? B. Recompiling the affected programs with the most current patches: While this can fix the immediate vulnerabilities, it does not address the root cause of the problem, which is the lack of regular updates.

? C. Disabling unused/unneeded ports on all servers: This improves security but does not address the specific issue of outdated software.

? D. Deploying a WAF with virtual patching upstream of the affected systems: This can provide a temporary shield but does not resolve the underlying issue of outdated software.

Automating the patching system to update base images ensures that all deployed systems are using the latest, most secure versions of software, addressing the root cause of the vulnerability trend.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-40 Rev. 3, "Guide to Enterprise Patch Management Technologies"

? CIS Controls, "Control 7: Continuous Vulnerability Management"

NEW QUESTION 55

A security analyst Detected unusual network traffic related to program updating processes The analyst collected artifacts from compromised user workstations. The discovered artifacts were binary files with the same name as existing, valid binaries but. with different hashes which of the following solutions would most likely prevent this situation from reoccurring?

- A. Improving patching processes
- B. Implementing digital signature
- C. Performing manual updates via USB ports
- D. Allowing only dies from internal sources

Answer: B

Explanation:

Implementing digital signatures ensures the integrity and authenticity of software binaries. When a binary is digitally signed, any tampering with the file (e.g., replacing it with a malicious version) would invalidate the signature. This allows systems to verify the origin and integrity of binaries before execution, preventing the execution of unauthorized or compromised binaries.

? A. Improving patching processes: While important, this does not directly address the issue of verifying the integrity of binaries.

? B. Implementing digital signatures: This ensures that only valid, untampered binaries are executed, preventing attackers from substituting legitimate binaries with malicious ones.

? C. Performing manual updates via USB ports: This is not practical and does not scale well, especially in large environments.

? D. Allowing only files from internal sources: This reduces the risk but does not provide a mechanism to verify the integrity of binaries.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-57, "Recommendation for Key Management"

? OWASP (Open Web Application Security Project) guidelines on code signing

NEW QUESTION 56

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 58

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 61

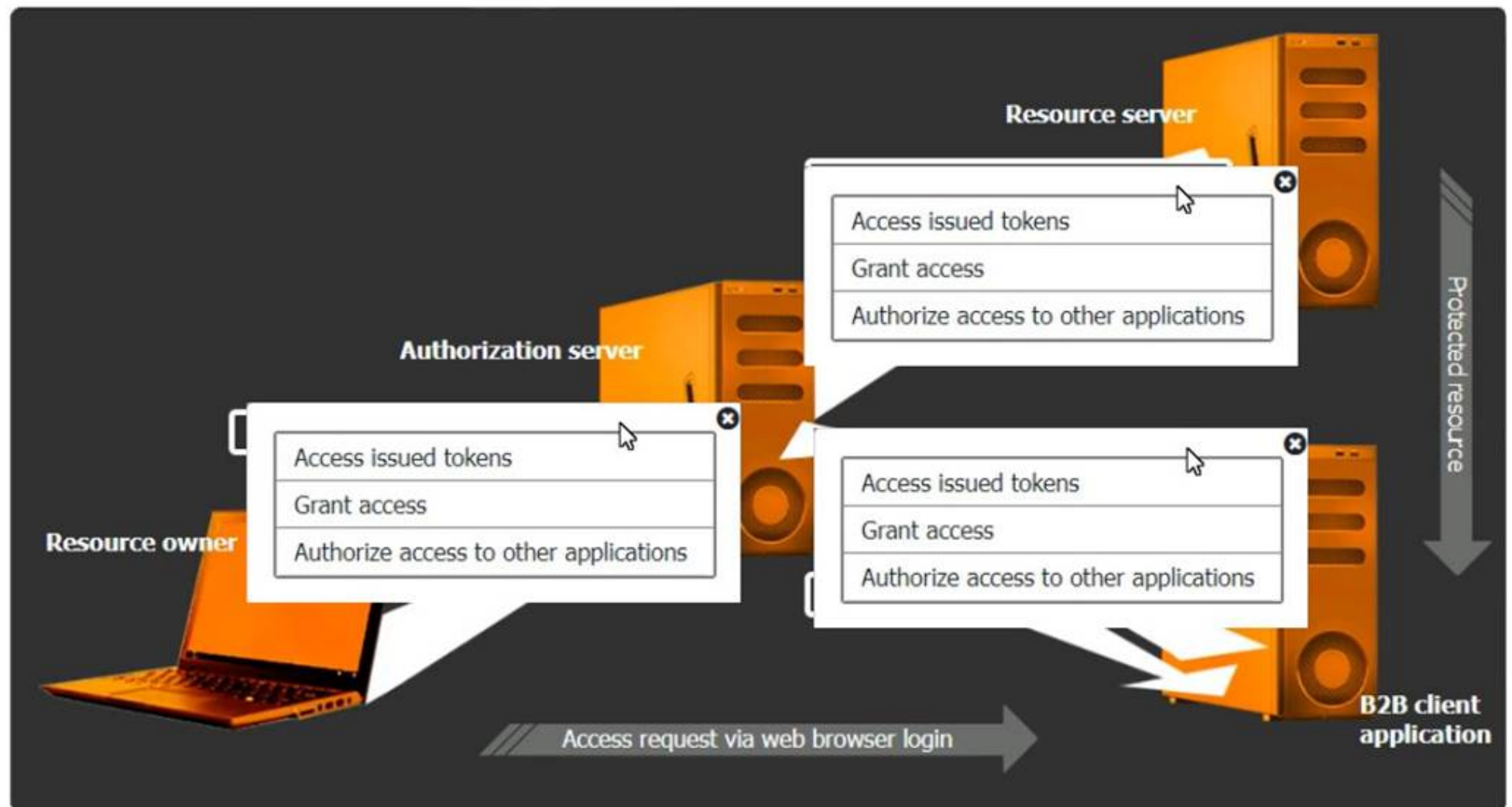
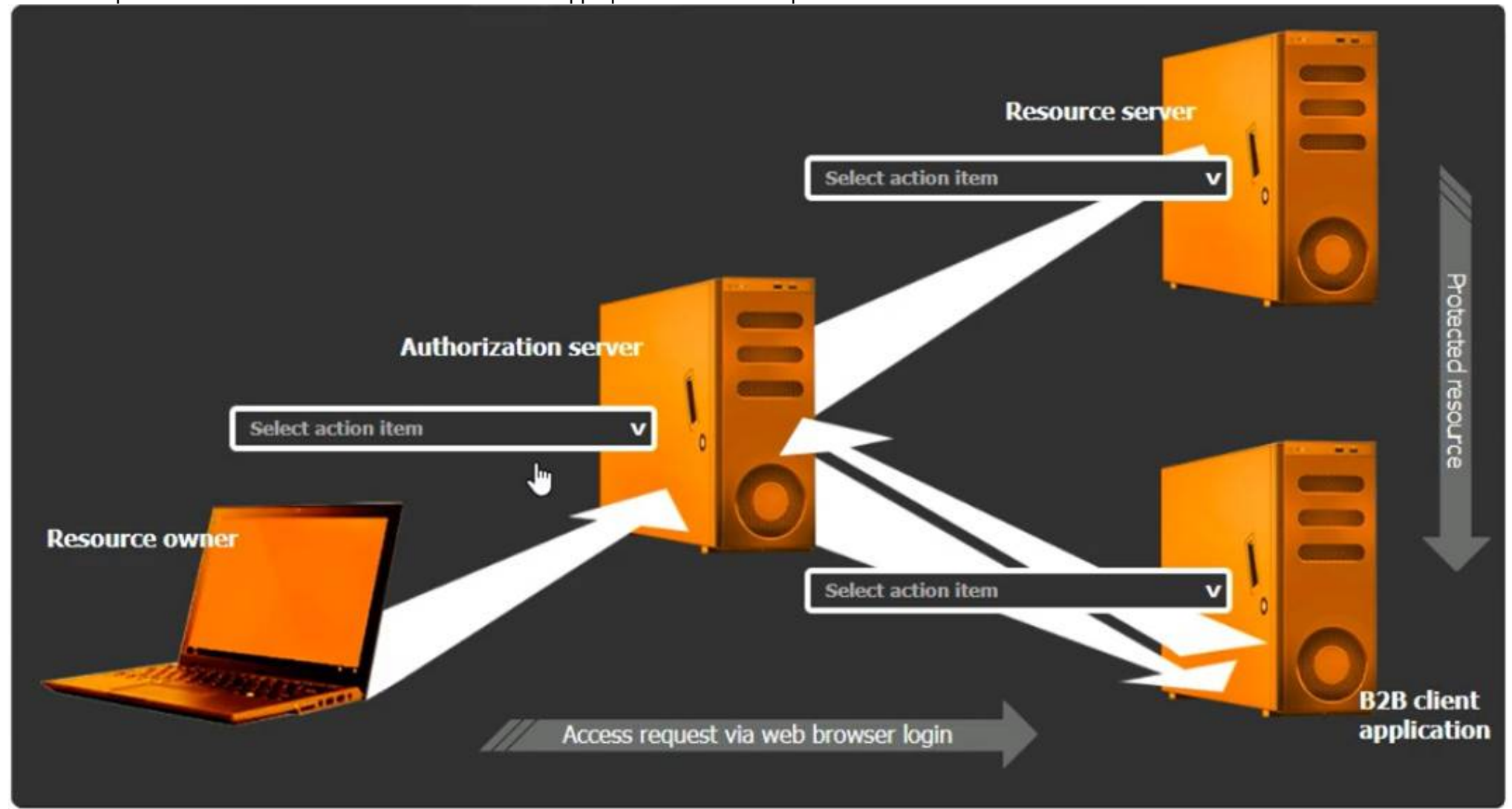
SIMULATION

You are tasked with integrating a new B2B client application with an existing OAuth workflow that must meet the following requirements:

- . The application does not need to know the users' credentials.
- . An approval interaction between the users and the HTTP service must be orchestrated.

. The application must have limited access to users' data. INSTRUCTIONS

Use the drop-down menus to select the action items for the appropriate locations. All placeholders must be filled.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Select the Action Items for the Appropriate Locations:

? Authorization Server:

? Resource Server:

? B2B Client Application:

Detailed Explanation

OAuth 2.0 is designed to provide specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. The integration involves multiple steps and components, including:

? Resource Owner (User):

? Client Application (B2B Client Application):

? Authorization Server:

? Resource Server:

OAuth Workflow:

? The resource owner accesses the client application.

? The client application redirects the resource owner to the authorization server for authentication.

? The authorization server authenticates the resource owner and asks for consent to grant access to the client application.

? Upon consent, the authorization server issues an authorization code or token to the client application.

? The client application uses the authorization code or token to request access to the resources from the resource server.

? The resource server verifies the token with the authorization server and, if valid, grants access to the requested resources.

References:

? CompTIA Security+ Study Guide: Provides comprehensive information on various authentication and authorization protocols, including OAuth.

? OAuth 2.0 Authorization Framework (RFC 6749): The official documentation detailing the OAuth 2.0 framework, its flows, and components.

? OAuth 2.0 Simplified: A book by Aaron Parecki that provides a detailed yet easy- to-understand explanation of the OAuth 2.0 protocol.

By ensuring that each component in the OAuth workflow performs its designated role, the B2B client application can securely access the necessary resources without compromising user credentials, adhering to the principle of least privilege.

NEW QUESTION 63

Which of the following best describes the challenges associated with widespread adoption of homomorphic encryption techniques?

A. Incomplete mathematical primitives

B. No use cases to drive adoption

C. Quantum computers not yet capable

D. insufficient coprocessor support

Answer: D

Explanation:

Homomorphic encryption allows computations to be performed on encrypted data without decrypting it, providing strong privacy guarantees. However, the adoption of homomorphic encryption is challenging due to several factors:

? A. Incomplete mathematical primitives: This is not the primary barrier as the theoretical foundations of homomorphic encryption are well-developed.

? B. No use cases to drive adoption: There are several compelling use cases for homomorphic encryption, especially in privacy-sensitive fields like healthcare and finance.

? C. Quantum computers not yet capable: Quantum computing is not directly related to the challenges of adopting homomorphic encryption.

? D. Insufficient coprocessor support: The computational overhead of homomorphic encryption is significant, requiring substantial processing power. Current general- purpose processors are not optimized for the intensive computations required by homomorphic encryption, limiting its practical deployment. Specialized hardware or coprocessors designed to handle these computations more efficiently are not yet widely available.

References:

? CompTIA Security+ Study Guide

? "Homomorphic Encryption: Applications and Challenges" by Rivest et al.

? NIST, "Report on Post-Quantum Cryptography"

NEW QUESTION 64

After remote desktop capabilities were deployed in the environment, various vulnerabilities were noticed.

- Exfiltration of intellectual property

- Unencrypted files

- Weak user passwords

Which of the following is the best way to mitigate these vulnerabilities? (Select two).

A. Implementing data loss prevention

B. Deploying file integrity monitoring

C. Restricting access to critical file services only

D. Deploying directory-based group policies

E. Enabling modem authentication that supports MFA

F. Implementing a version control system

G. Implementing a CMDB platform

Answer: AE

Explanation:

To mitigate the identified vulnerabilities, the following solutions are most appropriate:

? A. Implementing data loss prevention (DLP): DLP solutions help prevent the unauthorized transfer of data outside the organization. This directly addresses the exfiltration of intellectual property by monitoring, detecting, and blocking sensitive data transfers.

? E. Enabling modern authentication that supports Multi-Factor Authentication

(MFA): This significantly enhances security by requiring additional verification methods beyond just passwords. It addresses the issue of weak user passwords by making it much harder for unauthorized users to gain access, even if they obtain the password.

Other options, while useful in specific contexts, do not address all the vulnerabilities mentioned:

? B. Deploying file integrity monitoring helps detect changes to files but does not prevent data exfiltration or address weak passwords.

? C. Restricting access to critical file services improves security but is not comprehensive enough to mitigate all identified vulnerabilities.

? D. Deploying directory-based group policies can enforce security policies but might not directly prevent data exfiltration or ensure strong authentication.

? F. Implementing a version control system helps manage changes to files but is not a security measure for preventing the identified vulnerabilities.

? G. Implementing a CMDB platform (Configuration Management Database) helps manage IT assets but does not address the specific security issues mentioned.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"

? CIS Controls, "Control 13: Data Protection" and "Control 16: Account Monitoring and Control"

NEW QUESTION 67

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 69

A security administrator is performing a gap assessment against a specific OS benchmark. The benchmark requires the following configurations be applied to endpoints:

- Full disk encryption
- * Host-based firewall
- Time synchronization
- * Password policies
- Application allow listing
- * Zero Trust application access

Which of the following solutions best addresses the requirements? (Select two).

- A. CASB
- B. SBoM
- C. SCAP
- D. SASE
- E. HIDS

Answer: CD

Explanation:

To address the specific OS benchmark configurations, the following solutions are most appropriate:

* C. SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies.

* D. SASE (Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant access to applications and data.

These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.

References:

? CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures.

? NIST Special Publication 800-126, "The Technical Specification for the Security Content Automation Protocol (SCAP)": Details SCAP's role in security automation.

? "Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth: Covers the principles of Zero Trust and how SASE can implement them.

By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintained effectively.

NEW QUESTION 72

A software development team requires valid data for internal tests. Company regulations, however, do not allow the use of this data in cleartext. Which of the following solutions best meet these requirements?

- A. Configuring data hashing
- B. Deploying tokenization
- C. Replacing data with null record
- D. Implementing data obfuscation

Answer: B

Explanation:

Tokenization replaces sensitive data elements with non-sensitive equivalents, called tokens, that can be used within the internal tests. The original data is stored securely and can be retrieved if necessary. This approach allows the software development team to work with data that appears realistic and valid without exposing the actual sensitive information.

Configuring data hashing (Option A) is not suitable for test data as it transforms the data into a fixed-length value that is not usable in the same way as the original data. Replacing

data with null records (Option C) is not useful as it does not provide valid data for testing. Data obfuscation (Option D) could be an alternative but might not meet the regulatory requirements as effectively as tokenization.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-57 Part 1 Rev. 5, "Recommendation for Key Management"

? PCI DSS Tokenization Guidelines

NEW QUESTION 75

A cybersecurity architect is reviewing the detection and monitoring capabilities for a global company that recently made multiple acquisitions. The architect discovers that the acquired companies use different vendors for detection and monitoring. The architect's goal is to:

- Create a collection of use cases to help detect known threats
- Include those use cases in a centralized library for use across all of the companies. Which of the following is the best way to achieve this goal?

- A. Sigma rules
- B. Ariel Query Language
- C. UBA rules and use cases
- D. TAXII/STIX library

Answer: A

Explanation:

To create a collection of use cases for detecting known threats and include them in a centralized library for use across multiple companies with different vendors, Sigma rules are the best option. Here's why:

? Vendor-Agnostic Format: Sigma rules are a generic and open standard for writing

SIEM (Security Information and Event Management) rules. They can be translated to specific query languages of different SIEM systems, making them highly versatile and applicable across various platforms.

? Centralized Rule Management: By using Sigma rules, the cybersecurity architect

can create a centralized library of detection rules that can be easily shared and implemented across different detection and monitoring systems used by the acquired companies. This ensures consistency in threat detection capabilities.

? Ease of Use and Flexibility: Sigma provides a structured and straightforward

format for defining detection logic. It allows for the easy creation, modification, and sharing of rules, facilitating collaboration and standardization across the organization.

NEW QUESTION 77

An organization wants to manage specialized endpoints and needs a solution that provides the ability to

- * Centrally manage configurations
- * Push policies.

- Remotely wipe devices
- Maintain asset inventory

Which of the following should the organization do to best meet these requirements?

- A. Use a configuration management database
- B. Implement a mobile device management solution.
- C. Configure contextual policy management
- D. Deploy a software asset manager

Answer: B

Explanation:

To meet the requirements of centrally managing configurations, pushing policies, remotely wiping devices, and maintaining an asset inventory, the best solution is to implement a Mobile Device Management (MDM) solution.

MDM Capabilities:

? Central Management: MDM allows administrators to manage the configurations of all devices from a central console.

? Policy Enforcement: MDM solutions enable the push of security policies and updates to ensure compliance across all managed devices.

? Remote Wipe: In case a device is lost or stolen, MDM provides the capability to remotely wipe the device to protect sensitive data.

? Asset Inventory: MDM maintains an up-to-date inventory of all managed devices, including their configurations and installed applications.

Other options do not provide the same comprehensive capabilities required for managing specialized endpoints.

References:

? CompTIA SecurityX Study Guide

? NIST Special Publication 800-124 Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise"

? "Mobile Device Management Overview," Gartner Research

NEW QUESTION 79

A security analyst is troubleshooting the reason a specific user is having difficulty accessing company resources. The analyst reviews the following information:

User	Source IP	Source location	User assigned location	MFA satisfied?	Sign-in status
SALES1	8.11.4.16	Germany	France	Yes	Blocked
SALES1	8.11.4.16	Germany	France	Yes	Blocked
ACCT1	192.168.4.18	France	France	No	Allowed
SALES1	8.11.4.16	Germany	France	Yes	Blocked
ACCT1	8.11.4.16	Germany	France	Yes	Blocked
SALES2	8.11.4.20	France	France	Yes	Allowed

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

- A. The local network access has been configured to bypass MFA requirements.
- B. A network geolocation is being misidentified by the authentication server
- C. Administrator access from an alternate location is blocked by company policy
- D. Several users have not configured their mobile devices to receive OTP codes

Answer: B

Explanation:

The table shows that the user "SALES1" is consistently blocked despite having met the MFA requirements. The common factor in these blocked attempts is the source IP address (8.11.4.16) being identified as from Germany while the user is assigned to France. This discrepancy suggests that the network geolocation is being misidentified by the authentication server, causing legitimate access attempts to be blocked.

Why Network Geolocation Misidentification?

? Geolocation Accuracy: Authentication systems often use IP geolocation to verify the location of access attempts. Incorrect geolocation data can lead to legitimate requests being denied if they appear to come from unexpected locations.

? Security Policies: Company security policies might block access attempts from certain locations to prevent unauthorized access. If the geolocation is wrong, legitimate users can be inadvertently blocked.

? Consistent Pattern: The user "SALES1" from the IP address 8.11.4.16 is always blocked, indicating a consistent issue with geolocation.

Other options do not align with the pattern observed:

? A. Bypass MFA requirements: MFA is satisfied, so bypassing MFA is not the issue.

? C. Administrator access policy: This is about user access, not specific administrator access.

? D. OTP codes: The user has satisfied MFA, so OTP code configuration is not the issue.

References:

? CompTIA SecurityX Study Guide

? "Geolocation and Authentication," NIST Special Publication 800-63B

? "IP Geolocation Accuracy," Cisco Documentation

NEW QUESTION 84

A systems administrator wants to reduce the number of failed patch deployments in an organization. The administrator discovers that system owners modify systems or applications in an ad hoc manner. Which of the following is the best way to reduce the number of failed patch deployments?

- A. Compliance tracking
- B. Situational awareness
- C. Change management
- D. Quality assurance

Answer: C

Explanation:

To reduce the number of failed patch deployments, the systems administrator should implement a robust change management process. Change management ensures that all modifications to systems or applications are planned, tested, and approved before deployment. This systematic approach reduces the risk of unplanned changes that can cause patch failures and ensures that patches are deployed in a controlled and predictable manner.

References:

? CompTIA SecurityX Study Guide: Emphasizes the importance of change management in maintaining system integrity and ensuring successful patch deployments.

? ITIL (Information Technology Infrastructure Library) Framework: Provides best practices for change management in IT services.

? "The Phoenix Project" by Gene Kim, Kevin Behr, and George Spafford: Discusses the critical role of change management in IT operations and its impact on system stability and reliability.

NEW QUESTION 86

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 87

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 89

A network engineer must ensure that always-on VPN access is enabled and restricted to company assets. Which of the following best describes what the engineer needs to do?

- A. Generate device certificates using the specific template settings needed
- B. Modify signing certificates in order to support IKE version 2
- C. Create a wildcard certificate for connections from public networks
- D. Add the VPN hostname as a SAN entry on the root certificate

Answer: A

Explanation:

To ensure always-on VPN access is enabled and restricted to company assets, the network engineer needs to generate device certificates using the specific template settings required for the company's VPN solution. These certificates ensure that only authorized devices can establish a VPN connection.

Why Device Certificates are Necessary:

? Authentication: Device certificates authenticate company assets, ensuring that only authorized devices can access the VPN.

? Security: Certificates provide a higher level of security compared to username and password combinations, reducing the risk of unauthorized access.

? Compliance: Certificates help in meeting security policies and compliance requirements by ensuring that only managed devices can connect to the corporate network.

Other options do not provide the same level of control and security for always-on VPN access:

? B. Modify signing certificates for IKE version 2: While important for VPN protocols, it does not address device-specific authentication.

? C. Create a wildcard certificate: This is not suitable for device-specific authentication and could introduce security risks.

? D. Add the VPN hostname as a SAN entry: This is more related to certificate management and does not ensure device-specific authentication.

References:

? CompTIA SecurityX Study Guide

? "Device Certificates for VPN Access," Cisco Documentation

? NIST Special Publication 800-77, "Guide to IPsec VPNs"

NEW QUESTION 90

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 94

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 99

A company isolated its OT systems from other areas of the corporate network These systems are required to report usage information over the internet to the vendor Which oi the following b*st reduces the risk of compromise or sabotage' (Select two).

- A. Implementing allow lists
- B. Monitoring network behavior
- C. Encrypting data at rest
- D. Performing boot Integrity checks
- E. Executing daily health checks
- F. Implementing a site-to-site IPSec VPN

Answer: AF

Explanation:

? A. Implementing allow lists: Allow lists (whitelisting) restrict network communication to only authorized devices and applications, significantly reducing the attack surface by ensuring that only pre-approved traffic is permitted.

? F. Implementing a site-to-site IPSec VPN: A site-to-site VPN provides a secure, encrypted tunnel for data transmission between the OT systems and the vendor, protecting the data from interception and tampering during transit.

Other options:

? B. Monitoring network behavior: While useful for detecting anomalies, it does not proactively reduce the risk of compromise or sabotage.

? C. Encrypting data at rest: Important for protecting data stored on devices, but does not address network communication risks.

? D. Performing boot integrity checks: Ensures the integrity of the system at startup but does not protect ongoing network communications.

? E. Executing daily health checks: Useful for maintaining system health but does not directly reduce the risk of network-based compromise or sabotage.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security"

? "Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill

NEW QUESTION 101

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 104

During a gap assessment, an organization notes that OYOD usage is a significant risk. The organization implemented administrative policies prohibiting BYOD usage. However, the organization has not implemented technical controls to prevent the unauthorized use of BYOD assets when accessing the organization's resources. Which of the following

solutions should the organization implement to b» « reduce the risk of OYOD devices? (Select two).

- A. Cloud IAM to enforce the use of token based MFA
- B. Conditional access, to enforce user-to-device binding
- C. NAC, to enforce device configuration requirements
- D. PA
- E. to enforce local password policies
- F. SD-WA
- G. to enforce web content filtering through external proxies
- H. DLP, to enforce data protection capabilities

Answer: BC

Explanation:

To reduce the risk of unauthorized BYOD (Bring Your Own Device) usage, the organization should implement Conditional Access and Network Access Control (NAC). Why Conditional Access and NAC?

? Conditional Access:

? Network Access Control (NAC):

Other options, while useful, do not address the specific need to control and secure BYOD devices effectively:

? A. Cloud IAM to enforce token-based MFA: Enhances authentication security but

does not control device compliance.

? D. PAM to enforce local password policies: Focuses on privileged account management, not BYOD control.

? E. SD-WAN to enforce web content filtering: Enhances network performance and security but does not enforce BYOD device compliance.

? F. DLP to enforce data protection capabilities: Protects data but does not control BYOD device access and compliance.

References:

? CompTIA SecurityX Study Guide

? "Conditional Access Policies," Microsoft Documentation

? "Network Access Control (NAC)," Cisco Documentation

NEW QUESTION 107

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 srvo1 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 112

A user reports application access issues to the help desk. The help desk reviews the logs for the user

Time	Internal IP	Public IP	IP geolocation	Application	Action
8:47 p.m.	192.168.1.5	104.18.16.29	Toronto	VPN	Allow
8:48 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:48 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Human resources system	Allow
8:49 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:52 p.m.	192.168.1.5	104.18.16.29	Toronto	Human resources system	Deny

Which of the following is most likely The reason for the issue?

- A. The user inadvertently tripped the impossible travel security rule in the SSO system.
- B. A threat actor has compromised the user's account and attempted to log in
- C. The user is not allowed to access the human resources system outside of business hours
- D. The user did not attempt to connect from an approved subnet

Answer: A

Explanation:

Based on the provided logs, the user has accessed various applications from different geographic locations within a very short timeframe. This pattern is indicative of the "impossible travel" security rule, a common feature in Single Sign-On (SSO) systems designed to detect and prevent fraudulent access attempts.

Analysis of Logs:

? At 8:47 p.m., the user accessed a VPN from Toronto.

? At 8:48 p.m., the user accessed email from Los Angeles.

? At 8:48 p.m., the user accessed the human resources system from Los Angeles.

? At 8:49 p.m., the user accessed email again from Los Angeles.

? At 8:52 p.m., the user attempted to access the human resources system from Toronto, which was denied.

These rapid changes in location are physically impossible and typically trigger security measures to prevent unauthorized access. The SSO system detected these inconsistencies and likely flagged the activity as suspicious, resulting in access denial. References:

? CompTIA SecurityX Study Guide

? NIST Special Publication 800-63B, "Digital Identity Guidelines"

? "Impossible Travel Detection," Microsoft Documentation

NEW QUESTION 113

A company updates its cloud-based services by saving infrastructure code in a remote repository. The code is automatically deployed into the development environment every time the code is saved to the repository. The developers express concern that the deployment often fails, citing minor code issues and occasional security control check failures in the development environment. Which of the following should a security engineer recommend to reduce the deployment failures? (Select two).

- A. Software composition analysis
- B. Pre-commit code linting
- C. Repository branch protection
- D. Automated regression testing
- E. Code submit authorization workflow
- F. Pipeline compliance scanning

Answer: BD

Explanation:

- ? B. Pre-commit code linting: Linting tools analyze code for syntax errors and adherence to coding standards before the code is committed to the repository. This helps catch minor code issues early in the development process, reducing the likelihood of deployment failures.
- ? D. Automated regression testing: Automated regression tests ensure that new code changes do not introduce bugs or regressions into the existing codebase. By running these tests automatically during the deployment process, developers can catch issues early and ensure the stability of the development environment.
- Other options:
- ? A. Software composition analysis: This helps identify vulnerabilities in third-party components but does not directly address code quality or deployment failures.
- ? C. Repository branch protection: While this can help manage the code submission process, it does not directly prevent deployment failures caused by code issues or security check failures.
- ? E. Code submit authorization workflow: This manages who can submit code but does not address the quality of the code being submitted.
- ? F. Pipeline compliance scanning: This checks for compliance with security policies but does not address syntax or regression issues.

References:

- ? CompTIA Security+ Study Guide
- ? "Continuous Integration and Continuous Delivery" by Jez Humble and David Farley
- ? OWASP (Open Web Application Security Project) guidelines on secure coding practices

NEW QUESTION 114

After an incident response exercise, a security administrator reviews the following table:

Service	Risk rating	Criticality rating	Alert severity
Public website	Medium	Low	Low
Email	High	High	High
Human resources systems	High	Medium	Medium
Phone system	High	Critical	Critical
Intranet	Low	Low	Low

Which of the following should the administrator do to beat support rapid incident response in the future?

- A. Automate alerting to IT support for phone system outages.
- B. Enable dashboards for service status monitoring
- C. Send emails for failed log-in attempts on the public website
- D. Configure automated Isolation of human resources systems

Answer: B

Explanation:

Enabling dashboards for service status monitoring is the best action to support rapid incident response. The table shows various services with different risk, criticality, and alert severity ratings. To ensure timely and effective incident response, real-time visibility into the status of these services is crucial.

Why Dashboards for Service Status Monitoring?

- ? Real-time Visibility: Dashboards provide an at-a-glance view of the current status of all critical services, enabling rapid detection of issues.
- ? Centralized Monitoring: A single platform to monitor the status of multiple services helps streamline incident response efforts.
- ? Proactive Alerting: Dashboards can be configured to show alerts and anomalies immediately, ensuring that incidents are addressed as soon as they arise.
- ? Improved Decision Making: Real-time data helps incident response teams make informed decisions quickly, reducing downtime and mitigating impact.

Other options, while useful, do not offer the same level of comprehensive, real-time visibility and proactive alerting:

- ? A. Automate alerting to IT support for phone system outages: This addresses one service but does not provide a holistic view.
- ? C. Send emails for failed log-in attempts on the public website: This is a specific alert for one type of issue and does not cover all services.
- ? D. Configure automated isolation of human resources systems: This is a reactive measure for a specific service and does not provide real-time status monitoring.

References:

- ? CompTIA SecurityX Study Guide
- ? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"
- ? "Best Practices for Implementing Dashboards," Gartner Research

NEW QUESTION 118

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CAS-005 Practice Exam Features:

- * CAS-005 Questions and Answers Updated Frequently
- * CAS-005 Practice Questions Verified by Expert Senior Certified Staff
- * CAS-005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CAS-005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CAS-005 Practice Test Here](#)