CompTIA

Exam Questions CAS-005

CompTIA SecurityX Exam

NEW QUESTION 1
A company's help desk is experiencing a large number of calls from the finance department slating access issues to www bank com The security operations center reviewed the following security logs:

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

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

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

Answer: C

Explanation:
Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination. This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.
In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.
? Recursive DNS resolution failure (A) would generally lead to inability to resolve
DNS at all, not to a specific HTTP error.
? DNS poisoning (B) could result in users being directed to malicious sites, but again, would likely result in a different set of errors or unusual activity.
? Incorrect DNS setup (D) would likely cause broader resolution issues rather than targeted errors like the one seen here.
By reviewing the provided data, it is evident that the DNS traffic for www.bank.com is being rerouted improperly, resulting in consistent HTTP 495 errors for the finance department users. Hence, the most likely cause is that the DNS traffic is being sinkholed.
References:
? CompTIA SecurityX study materials on DNS security mechanisms.
? Standard HTTP status codes and their implications.

NEW QUESTION 2
Which of the following best explains the business requirement a healthcare provider fulfills by encrypting patient data at rest?

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

Answer: D

Explanation:
Encrypting patient data at rest is a critical requirement for healthcare providers to ensure compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The primary business requirement fulfilled by this practice is the protection of patient privacy while supporting the portability of medical information. By encrypting data at rest, healthcare providers safeguard sensitive patient information from unauthorized access, ensuring that privacy is maintained even if the storage media are compromised. Additionally, encryption supports the portability of patient records, allowing for secure transfer and access across different systems and locations while ensuring that privacy controls are in place.
References:
? CompTIA SecurityX Study Guide: Emphasizes the importance of data encryption for protecting sensitive information and ensuring compliance with regulatory requirements.
? HIPAA Security Rule: Requires healthcare providers to implement safeguards, including encryption, to protect patient data.
? "Health Informatics: Practical Guide for Healthcare and Information Technology Professionals" by Robert E. Hoyt: Discusses encryption as a key measure for protecting patient data privacy and supporting data portability.

NEW QUESTION 3
A company is having issues with its vulnerability management program New devices/IPs are added and dropped regularly, making the vulnerability report inconsistent Which of the following actions should the company lake to most likely improve the vulnerability management process'

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

Answer: D

Explanation:
To improve the vulnerability management process in an environment where new devices/IPs are added and dropped regularly, the company should perform regular discovery scanning throughout the IT landscape using the vulnerability management tool. Here??s why:
? Accurate Asset Inventory: Regular discovery scans help maintain an up-to-date

inventory of all assets, ensuring that the vulnerability management process includes all relevant devices and IPs.
? Consistency in Reporting: By continuously discovering and scanning new and
existing assets, the company can generate consistent and comprehensive vulnerability reports that reflect the current state of the network.
? Proactive Management: Regular scans enable the organization to proactively identify and address vulnerabilities on new and existing assets, reducing the window of exposure to potential threats.
? References:

NEW QUESTION 4
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 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 loCs.
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 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 7
A security analyst is reviewing the following log:

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

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

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

Answer: B

Explanation:
Based on the log provided, the most concerning event that should be investigated further is
the presence of a text file containing passwords that were leaked. Here's why:
? Sensitive Information Exposure: A text file containing passwords represents a significant security risk, as it indicates that sensitive credentials have been exposed in plain text, potentially leading to unauthorized access.
? Immediate Threat: Password leaks can lead to immediate exploitation by attackers, compromising user accounts and sensitive data. This requires urgent investi

NEW QUESTION 8
A global manufacturing company has an internal application mat is critical to making products This application cannot be updated and must Be available in the production area A security architect is implementing security for the application. Which of the following best describes the action the architect should take-?

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

Answer: D

Explanation:
Creating a separate network for users who need access to the application is the best action to secure an internal application that is critical to the production area and cannot be updated.
Why Separate Network?
? Network Segmentation: Isolates the critical application from the rest of the network, reducing the risk of compromise and limiting the potential impact of any security incidents.
? Controlled Access: Ensures that only authorized users have access to the application, enhancing security and reducing the attack surface.
? Minimized Risk: Segmentation helps in protecting the application from vulnerabilities that could be exploited from other parts of the network.
Other options, while beneficial, do not provide the same level of security for a critical application:
? A. Disallow wireless access: Useful but does not provide comprehensive protection.
? B. Deploy intrusion detection capabilities using a network tap: Enhances monitoring but does not provide the same level of isolation and control.
? C. Create an acceptable use policy: Important for governance but does not provide technical security controls.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-125, "Guide to Security for Full Virtualization Technologies"
? "Network Segmentation Best Practices," Cisco Documentation

NEW QUESTION 9
A user submits a help desk ticket stating then account does not authenticate sometimes. An analyst reviews the following logs for the user:
Which of the following best explains the reason the user's access is being denied?

A. incorrectly typed password
B. Time-based access restrictions
C. Account compromise
D. Invalid user-to-device bindings

Answer: B

Explanation:
The logs reviewed for the user indicate that access is being denied due to time-based access restrictions. These restrictions are commonly implemented to limit access to systems during specific hours to enhance security. If a user attempts to authenticate outside of the allowed time window, access will be denied. This measure helps prevent unauthorized access during non-business hours, reducing the risk of security incidents.
References:

? CompTIA SecurityX Study Guide: Covers various access control methods, including time-based restrictions, as a means of enhancing security.
? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations": Recommends the use of time-based access restrictions as part of access control policies.
? "Access Control and Identity Management" by Mike Chapple and Aaron French: Discusses the implementation and benefits of time-based access restrictions.

NEW QUESTION 10
A company wants to use loT devices to manage and monitor thermostats at all facilities The thermostats must receive vendor security updates and limit access to other devices within the organization Which of the following best addresses the company's requirements"

A. Only allowing Internet access to a set of specific domains
B. Operating lot devices on a separate network with no access to other devices internally
C. Only allowing operation for loT devices during a specified time window
D. Configuring IoT devices to always allow automatic updates

Answer: B

Explanation:
The best approach for managing and monitoring IoT devices, such as thermostats, is to operate them on a separate network with no access to other internal devices. This segmentation ensures that the IoT devices are isolated from the main network, reducing the risk of potential security breaches affecting other critical systems. Additionally, this setup allows for secure vendor updates without exposing the broader network to potential vulnerabilities inherent in IoT devices.
References:
? CompTIA SecurityX Study Guide: Recommends network segmentation for IoT devices to minimize security risks.
? NIST Special Publication 800-183, "Network of Things": Advises on the isolation of IoT devices to enhance security.
? "Practical IoT Security" by Brian Russell and Drew Van Duren: Discusses best practices for securing IoT devices, including network segmentation.

NEW QUESTION 10
During a security assessment using an CDR solution, a security engineer generates the following report about the assets in me system:

Device	Type	Status
LN002	Linux SE	Enabled (unmanaged)
0WIN23	Windows 7	Enabled
0WIN29	Windows 10	Enabled (bypass)

After five days, the EDR console reports an infection on the host 0WIN23 by a remote access Trojan Which of the following is the most probable cause of the infection?

A. OW1N23 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. 0W1N29 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 15
Which of the following is the main reason quantum computing advancements are leading companies and countries to deploy new encryption algorithms?

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

Answer: A

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

cryptographic systems vulnerable.
Why Large Prime Numbers are Vulnerable:
? Shor's Algorithm: Quantum computers can use Shor's algorithm to factorize large integers efficiently, which undermines the security of RSA encryption.
? Cryptographic Breakthrough: The ability to quickly factor large prime numbers means that encrypted data, which relies on the hardness of this mathematical problem, can be decrypted.
Other options, while relevant, do not capture the primary reason for the shift towards new encryption algorithms:
? B. Zero Trust security architectures: While important, the shift to homomorphic
encryption is not the main driver for new encryption algorithms.
? C. Perfect forward secrecy: It enhances security but is not the main reason for new encryption algorithms.
? D. Real-time IP traffic capture: Quantum computers pose a more significant threat to the underlying cryptographic algorithms than to the real-time capture of traffic.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-208, "Recommendation for Stateful Hash-Based Signature Schemes"
? "Quantum Computing and Cryptography," MIT Technology Review

NEW QUESTION 18
A security officer received several complaints from users about excessive MPA 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 MI~A notifications"

A. Provisioning FID02 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 20
Developers have been creating and managing cryptographic material on their personal laptops fix use in production environment. A security engineer needs to initiate a more secure process. Which of the following is the best strategy for the engineer to use?

A. Disabling the BIOS and moving to UEFI
B. Managing secrets on the vTPM hardware
C. Employing shielding lo 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 22
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 m 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 26
An organization is looking for gaps in its detection capabilities based on the APTs that may target the industry Which of the following should the security analyst use to perform threat modeling?

A. ATT&CK
B. OWASP
C. CAPEC
D. STRIDE

Answer: A

Explanation:
The ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is the best tool for a security analyst to use for threat modeling when looking for gaps in detection capabilities based on Advanced Persistent Threats (APTs) that may target the industry. Here??s why:
? Comprehensive Framework: ATT&CK provides a detailed and structured repository of known adversary tactics and techniques based on real-world observations. It helps organizations understand how attackers operate and what techniques they might use.
? Gap Analysis: By mapping existing security controls against the ATT&CK matrix, analysts can identify which tactics and techniques are not adequately covered by current detection and mitigation measures.
? Industry Relevance: The ATT&CK framework is continuously updated with the latest threat intelligence, making it highly relevant for industries facing APT threats. It provides insights into specific APT groups and their preferred methods of attack.
? References:

NEW QUESTION 31
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 34

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 37
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 40
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 41
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 44
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

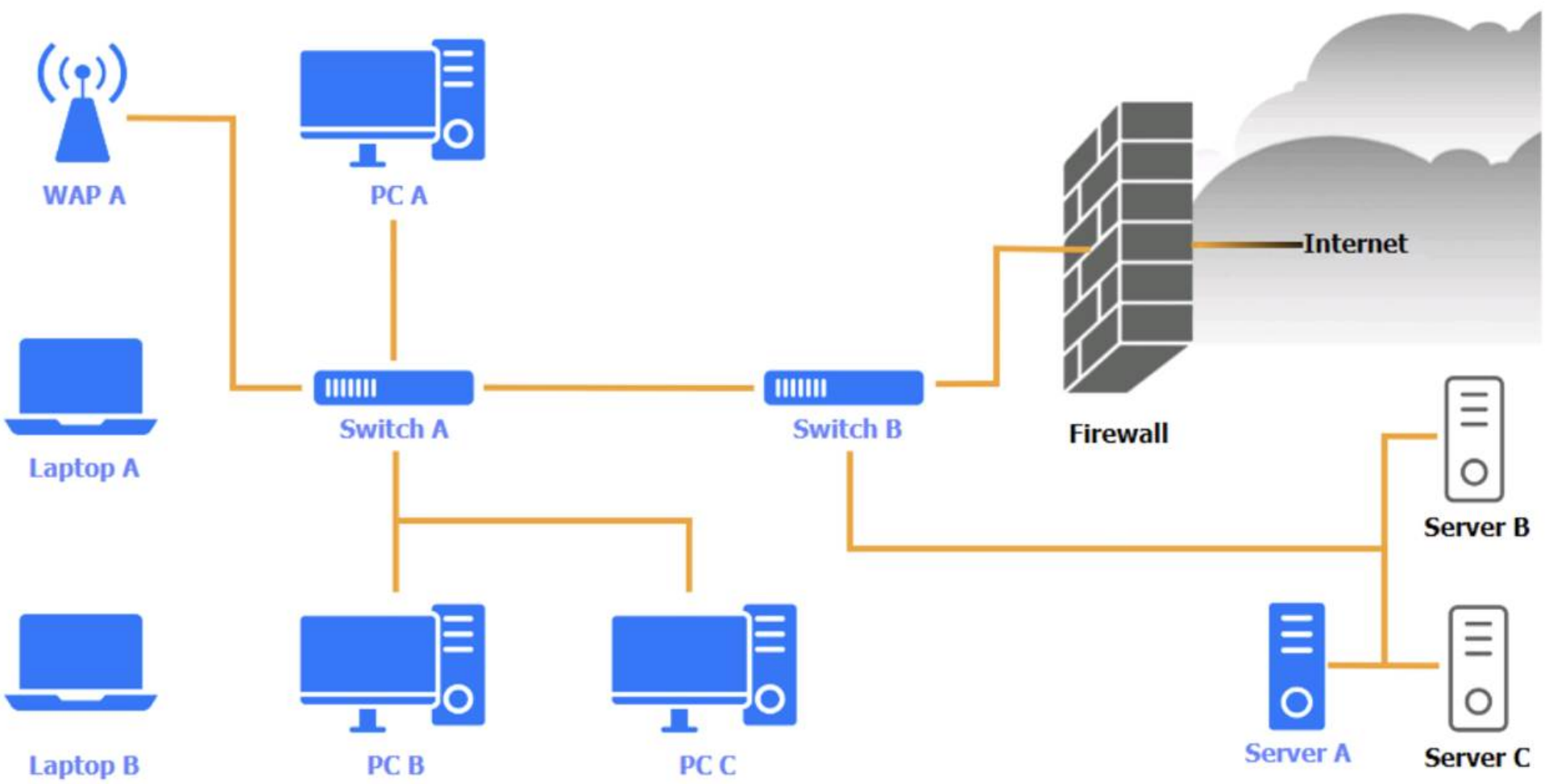
Which of the following assessments is the analyst performing?

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 46
SIMULATION
A security engineer needs to review the configurations of several devices on the network to meet the following requirements:
• The PostgreSQL server must only allow connectivity in the 10.1.2.0/24 subnet.
• The SSH daemon on the database server must be configured to listen to port 4022.
• The SSH daemon must only accept connections from a Single workstation.
• All host-based firewalls must be disabled on all workstations.
• All devices must have the latest updates from within the past eight days.
• All HDDs must be configured to secure data at rest.
• Cleartext services are not allowed.
• All devices must be hardened when possible.
Instructions:
Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found.
Click on Server A to review output data. Select commands in the appropriate tab to remediate connectivity problems to the pOSTGREsql DATABASE VIA ssh



WAP A

WAP A

Finding	Status	Remediation
Firmware	Updated 5 days ago	☑ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
SSID broadcast	Disabled	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
HTTP server	Disabled	☐ Enable port security on network device
		☐ Enable password complexity
		☐ Enable host-based firewall to block all traffic
		☐ Antivirus scan
		☐ Change default administrative password
		☐ Disable unneeded services
		☐ Enable all connectivity settings

PC A

PC A

OS updates	Updated 2 days ago, last checked 5:08 a.m.
Endpoint protection	Last checked 6:11 a.m.
Browser version	91.2.5 (7/31/2023)
Disk encryption	Enabled
Password complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Normal
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 389, 53
Wireless	Disabled

- [x] No issue
- [ ] Patch management
- [ ] Update endpoint protection
- [ ] Enabled disk encryption
- [ ] Enable port security on network device
- [ ] Enable password complexity
- [ ] Enable host-based firewall to block all traffic
- [ ] Antivirus scan
- [ ] Change default administrative password
- [ ] Disable unneeded services
- [ ] Enable all connectivity settings

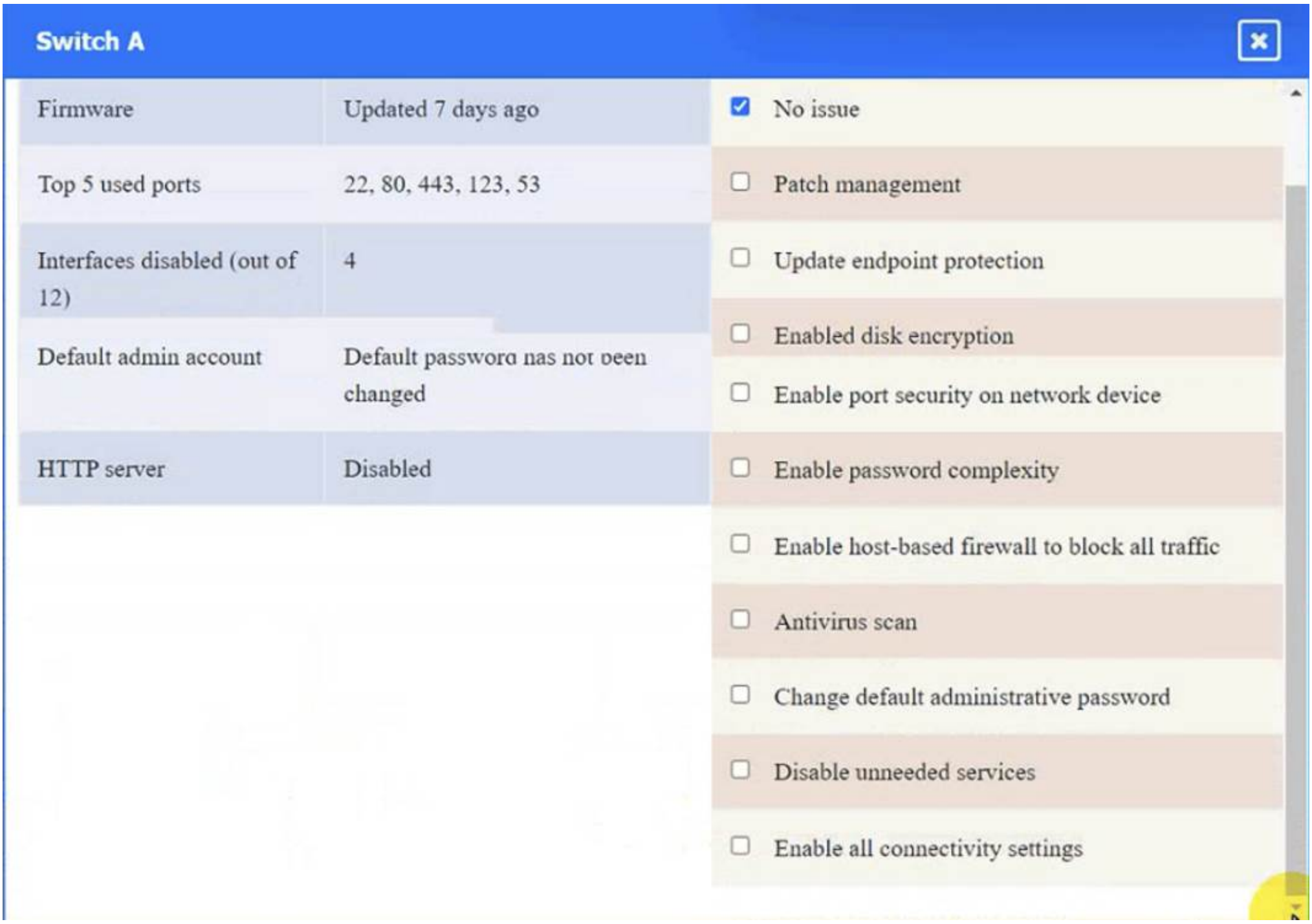
Laptop A

Laptop A

OS updates	Updated 3 days ago, last checked 6:08 a.m.
Endpoint protection	Last checked in 6:13 a.m.
Browser version	91.2.5 (7/31/2023)
Disk encryption	Enabled
Password complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Medium
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 389, 53
Wireless	Enabled

- [x] No issue
- [ ] Patch management
- [ ] Update endpoint protection
- [ ] Enabled disk encryption
- [ ] Enable port security on network device
- [ ] Enable password complexity
- [ ] Enable host-based firewall to block all traffic
- [ ] Antivirus scan
- [ ] Change default administrative password
- [ ] Disable unneeded services
- [ ] Enable all connectivity settings

Switch A



Switch B:

Switch B

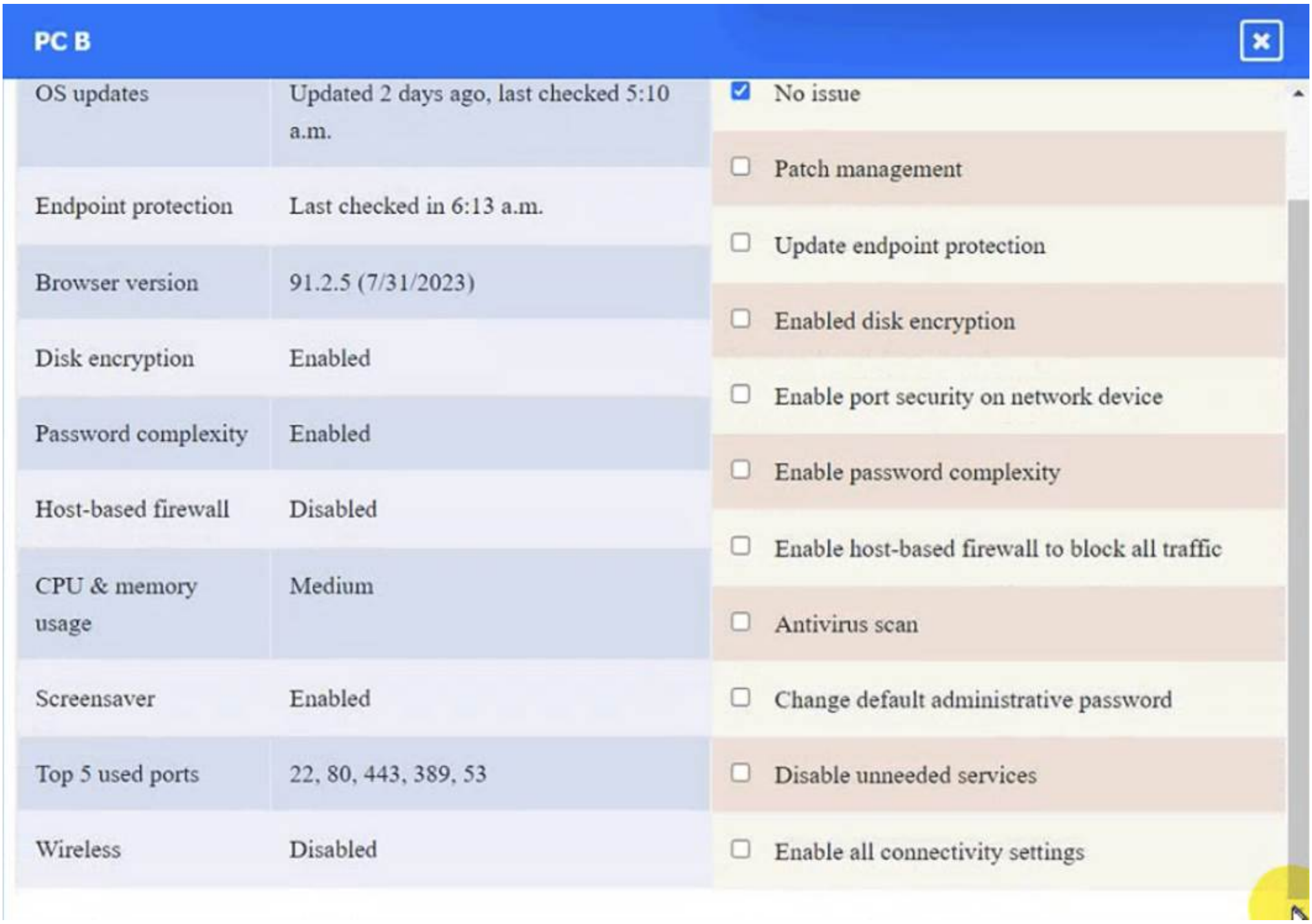
Firmware	Updated 7 days ago	☑ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
Interfaces disabled (out of 6)	1	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
		☐ Enable port security on network device
HTTP server	Disabled	☐ Enable password complexity
		☐ Enable host-based firewall to block all traffic
		☐ Antivirus scan
		☐ Change default administrative password
		☐ Disable unneeded services
		☐ Enable all connectivity settings

Laptop B

Laptop B

OS updates	Updated 3 days ago, last checked 8:08 a.m.	☑ No issue
Endpoint protection	Last checked in 8:11 a.m.	☐ Patch management
Browser version	81.2.5 (7/31/2023)	☐ Update endpoint protection
Disk encryption	Disabled	☐ Enabled disk encryption
		☐ Enable port security on network device
Password Complexity	Enabled	☐ Enable password complexity
Host-based firewall	Disabled	☐ Enable host-based firewall to block all traffic
CPU & memory usage	Normal	☐ Antivirus scan
		☐ Change default administrative password
Screensaver	Enabled	☐ Disable unneeded services
Top 5 used ports	22, 80, 443, 8080, 53	☐ Enable all connectivity settings
Wireless	Enabled	

PC B


PC B
OS updates
Updated 2 days ago, last checked 5:10 a.m.
Endpoint protection
Last checked in 6:13 a.m.
Browser version
91.2.5 (7/31/2023)
Disk encryption
Enabled
Password complexity
Enabled
Host-based firewall
Disabled
CPU & memory usage
Medium
Screensaver
Enabled
Top 5 used ports
22, 80, 443, 389, 53
Wireless
Disabled
No issue
Patch management
Update endpoint protection
Enabled disk encryption
Enable port security on network device
Enable password complexity
Enable host-based firewall to block all traffic
Antivirus scan
Change default administrative password
Disable unneeded services
Enable all connectivity settings

PC C


PC C
OS updates
Updated 22 days ago
Endpoint protection
Last checked 6:19 a.m.
Browser version
91.2.5 (7/18/2022)
Disk encryption
Enabled
Password complexity
Enabled
Host-based firewall
Disabled
CPU & memory usage
High
Screensaver
Enabled
Top 5 used ports
22, 80, 443, 23, 53
Wireless
Disabled
No issue
Patch management
Update endpoint protection
Enabled disk encryption
Enable port security on network device
Enable password complexity
Enable host-based firewall to block all traffic
Antivirus scan
Change default administrative password
Disable unneeded services
Enable all connectivity settings

Server A

Server A

Nmap | IP Tables

```
Nmap scan report for psql-srvr.acme.com
Host is up, received arp-response (0.00040s latency).
...
PORT            STATE   SERVICE         VERSION
22/tcp          open    ssh             OpenSSH 8.4
80/tcp          closed  http
443/tcp         closed  ssl/http
1433/tcp        closed  mssql
5432/tcp        closed  postgresql
...
```

1 2 3 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p udp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

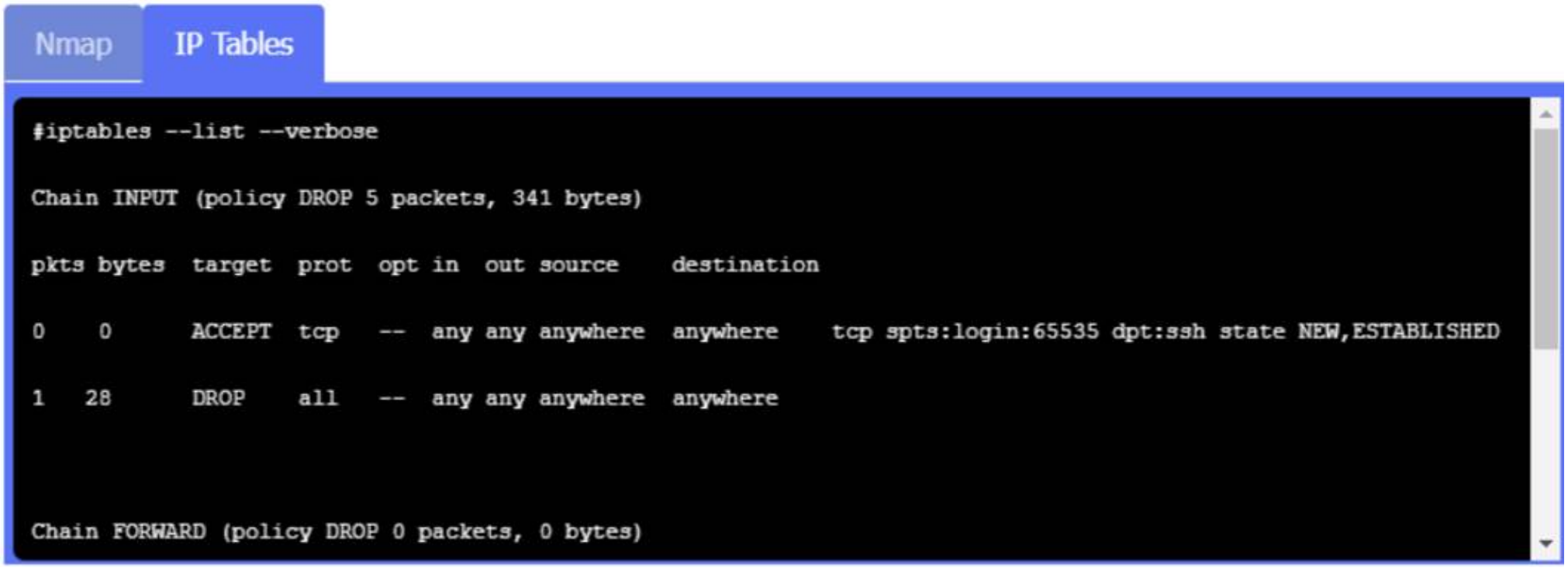
```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R OUTPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -F OUTPUT
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

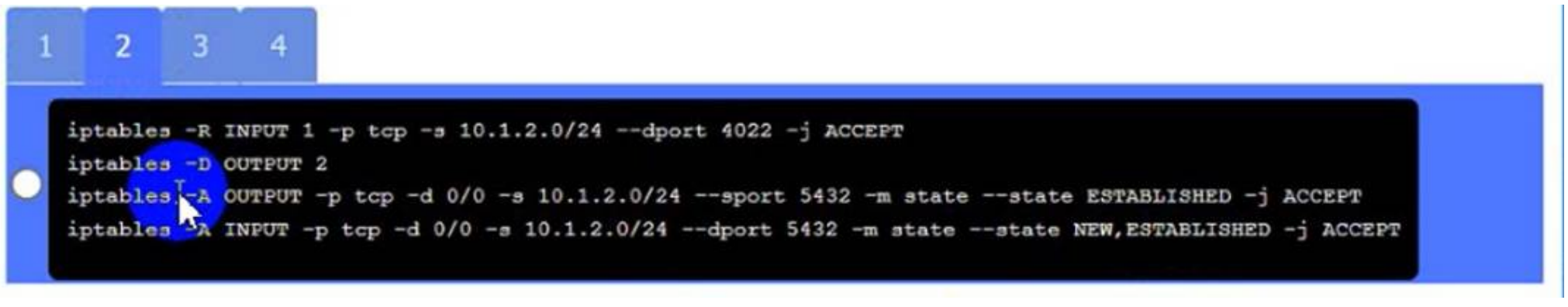
```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --dport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```



A. Mastered
B. Not Mastered

Answer: A

Explanation:
WAP A: No issue found. The WAP A is configured correctly and meets the requirements. PC A = Enable host-based firewall to block all traffic
This option will turn off the host-based firewall and allow all traffic to pass through. This will comply with the requirement and also improve the connectivity of PC A to other devices on the network. However, this option will also reduce the security of PC A and make it more vulnerable to attacks. Therefore, it is recommended to use other security measures, such as antivirus, encryption, and password complexity, to protect PC A from potential threats.
Laptop A: Patch management
This option will install the updates that are available for Laptop A and ensure that it has the most recent security patches and bug fixes. This will comply with the requirement and also improve the performance and stability of Laptop A. However, this option may also require a reboot of Laptop A and some downtime during the update process. Therefore, it is recommended to backup any important data and close any open applications before applying the updates.
Switch A: No issue found. The Switch A is configured correctly and meets the requirements.
Switch B: No issue found. The Switch B is configured correctly and meets the requirements.
Laptop B: Disable unneeded services
This option will stop and disable the telnet service that is using port 23 on Laptop B. Telnet
is a cleartext service that transmits data in plain text over the network, which exposes it to eavesdropping, interception, and modification by attackers. By disabling the telnet service, you will comply with the requirement and also improve the security of Laptop B. However, this option may also affect the functionality of Laptop B if it needs to use telnet for remote administration or other purposes. Therefore, it is recommended to use a secure alternative to telnet, such as SSH or HTTPS, that encrypts the data in transit.
PC B: Enable disk encryption
This option will encrypt the HDD of PC B using a tool such as BitLocker or VeraCrypt. Disk encryption is a technique that protects data at rest by converting it into an unreadable format that can only be decrypted with a valid key or password. By enabling disk encryption, you will comply with the requirement and also improve the confidentiality and integrity of PC B??s data. However, this option may also affect the performance and usability of PC B, as it requires additional processing time and user authentication to access the encrypted data. Therefore, it is recommended to backup any important data and choose a strong key or password before encrypting the disk.
PC C: Disable unneeded services
This option will stop and disable the SSH daemon that is using port 22 on PC C. SSH is a secure service that allows remote access and command execution over an encrypted channel. However, port 22 is the default and well-known port for SSH, which makes it a common target for brute-force attacks and port scanning. By disabling the SSH daemon on port 22, you will comply with the requirement and also improve the security of PC C. However, this option may also affect the functionality of PC C if it needs to use SSH for remote administration or other purposes. Therefore, it is recommended to enable the SSH daemon on a different port, such as 4022, by editing the configuration file using the following command:
sudo nano /etc/ssh/sshd_config Server A. Need to select the following:
white screen with white text



NEW QUESTION 49
A financial technology firm works collaboratively with business partners in the industry to share threat intelligence within a central platform This collaboration gives partner organizations the ability to obtain and share data associated with emerging threats from a variety of adversaries Which of the following should the organization most likely leverage to facilitate this activity? (Select two).

A. CWPP
B. YAKA
C. ATTACK
D. STIX
E. TAXII

F. JTAG

Answer: DE

Explanation:
? D. STIX (Structured Threat Information eXpression): STIX is a standardized language for representing threat information in a structured and machine-readable format. It facilitates the sharing of threat intelligence by ensuring that data is consistent and can be easily understood by all parties involved.
? E. TAXII (Trusted Automated eXchange of Indicator Information): TAXII is a transport mechanism that enables the sharing of cyber threat information over a secure and trusted network. It works in conjunction with STIX to automate the exchange of threat intelligence among organizations.
Other options:
? A. CWPP (Cloud Workload Protection Platform): This focuses on securing cloud workloads and is not directly related to threat intelligence sharing.
? B. YARA: YARA is used for malware research and identifying patterns in files, but it is not a platform for sharing threat intelligence.
? C. ATT&CK: This is a knowledge base of adversary tactics and techniques but does not facilitate the sharing of threat intelligence data.
? F. JTAG: JTAG is a standard for testing and debugging integrated circuits, not related to threat intelligence.
References:
? CompTIA Security+ Study Guide
? "STIX and TAXII: The Backbone of Threat Intelligence Sharing" by MITRE
? NIST SP 800-150, "Guide to Cyber Threat Information Sharing"

NEW QUESTION 52
A company that uses containers to run its applications is required to identify vulnerabilities on every container image in a private repository The security team needs to be able to quickly evaluate whether to respond to a given vulnerability Which of the following, will allow the security team to achieve the objective with the last effort?

A. SAST scan reports
B. Centralized SBoM
C. CIS benchmark compliance reports
D. Credentialed vulnerability scan

Answer: B

Explanation:
A centralized Software Bill of Materials (SBoM) is the best solution for identifying vulnerabilities in container images in a private repository. An SBoM provides a comprehensive inventory of all components, dependencies, and their versions within a container image, facilitating quick evaluation and response to vulnerabilities.
Why Centralized SBoM?
? Comprehensive Inventory: An SBoM lists all software components, including their versions and dependencies, allowing for thorough vulnerability assessments.
? Quick Identification: Centralizing SBoM data enables rapid identification of affected containers when a vulnerability is disclosed.
? Automation: SBoMs can be integrated into automated tools for continuous monitoring and alerting of vulnerabilities.
? Regulatory Compliance: Helps in meeting compliance requirements by providing a clear and auditable record of all software components used.
Other options, while useful, do not provide the same level of comprehensive and efficient vulnerability management:
? A. SAST scan reports: Focuses on static analysis of code but may not cover all components in container images.
? C. CIS benchmark compliance reports: Ensures compliance with security benchmarks but does not provide detailed component inventory.
? D. Credentialed vulnerability scan: Useful for in-depth scans but may not be as efficient for quick vulnerability evaluation.
References:
? CompTIA SecurityX Study Guide
? "Software Bill of Materials (SBoM)," NIST Documentation
? "Managing Container Security with SBoM," OWASP

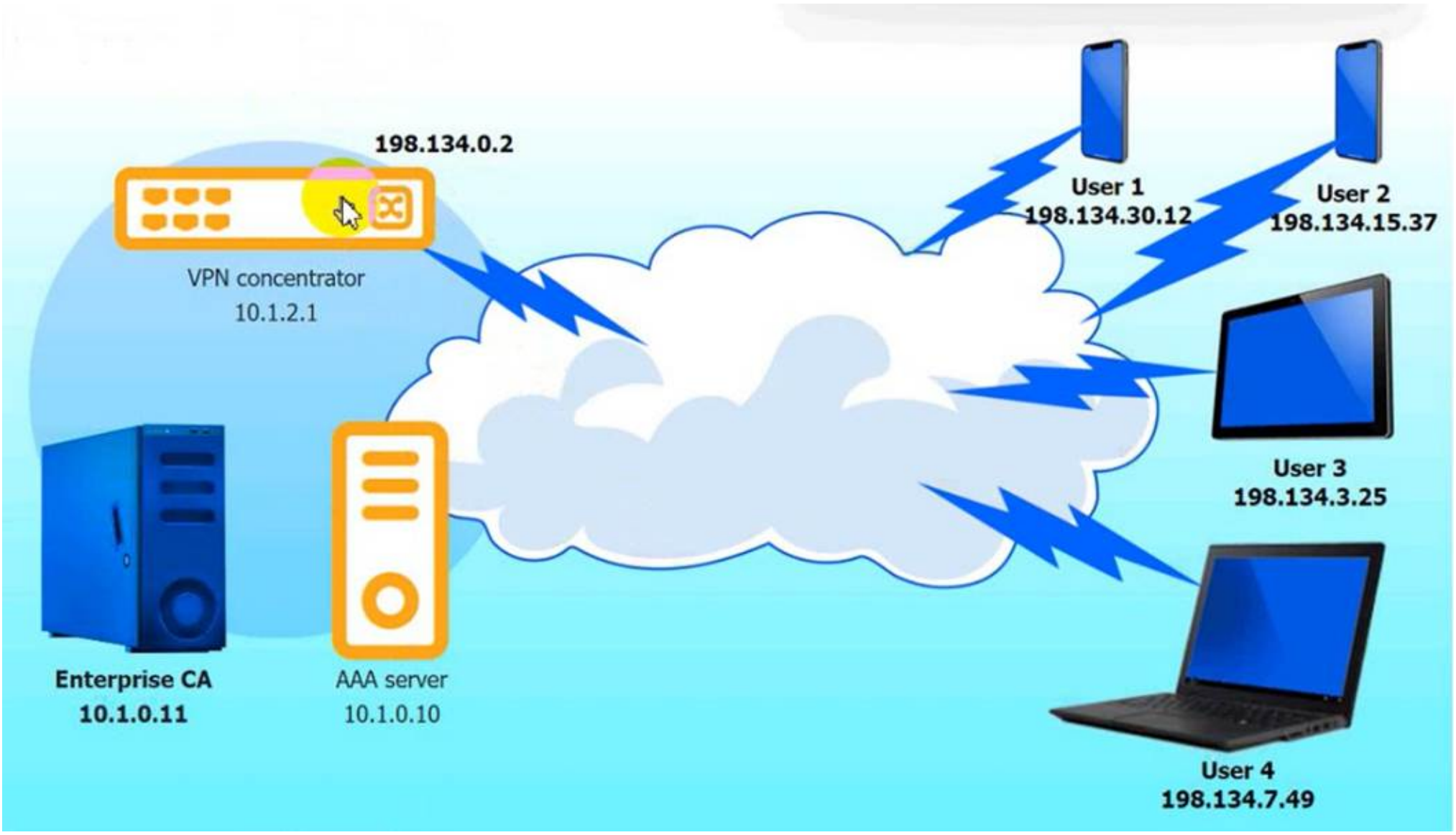
NEW QUESTION 53
A security team is responding to malicious activity and needs to determine the scope of impact the malicious activity appears to affect certain version of an application used by the organization Which of the following actions best enables the team to determine the scope of Impact?

A. Performing a port scan
B. Inspecting egress network traffic
C. Reviewing the asset inventory
D. Analyzing user behavior

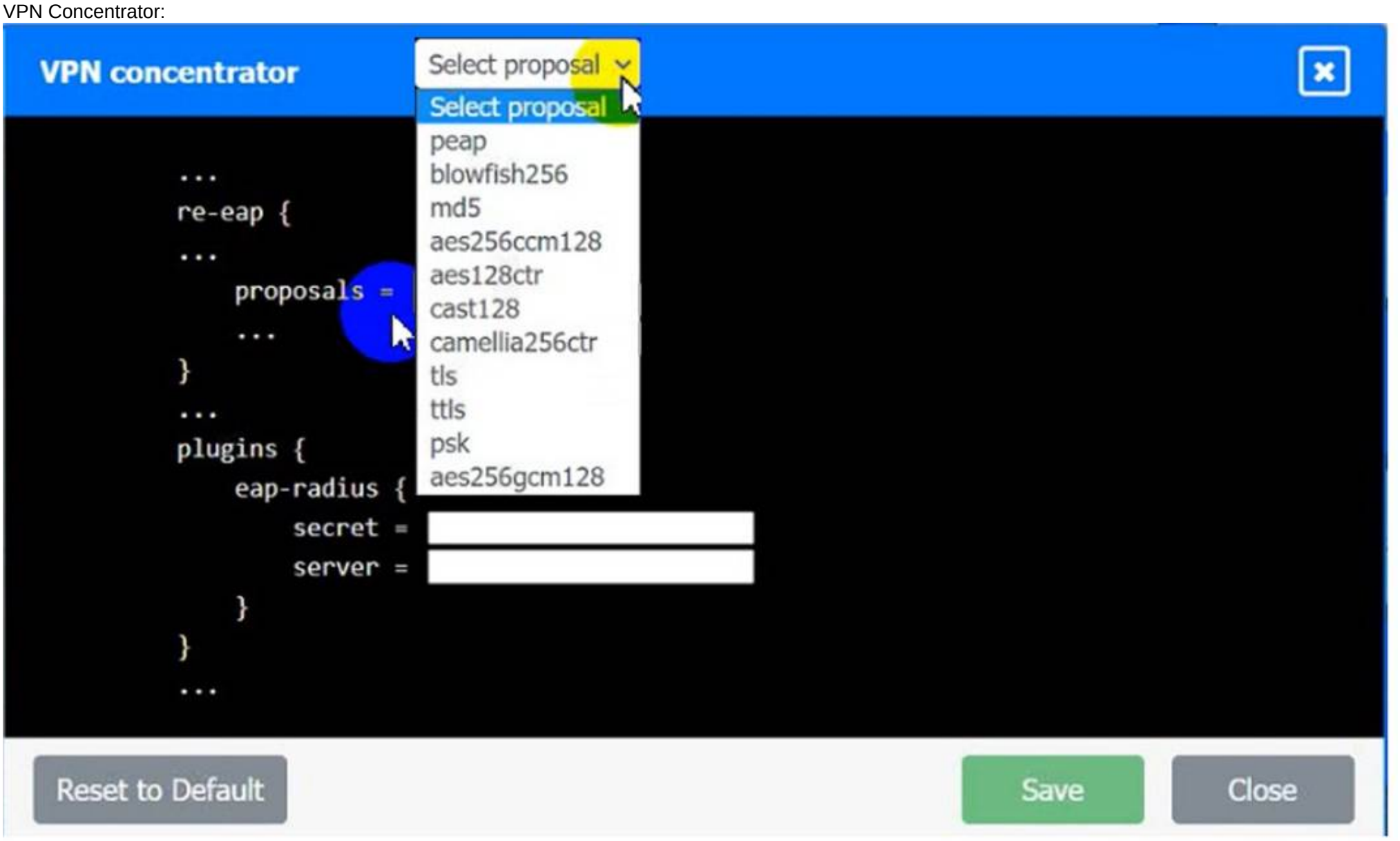
Answer: C

Explanation:
Reviewing the asset inventory allows the security team to identify all instances of the affected application versions within the organization. By knowing which systems are running the vulnerable versions, the team can assess the full scope of the impact, determine which systems might be compromised, and prioritize them for further investigation and remediation.
Performing a port scan (Option A) might help identify open ports but does not provide specific information about the application versions. Inspecting egress network traffic (Option B) and analyzing user behavior (Option D) are important steps in the incident response process but do not directly identify which versions of the application are affected. References:
? CompTIA Security+ Study Guide
? NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"
? CIS Controls, "Control 1: Inventory and Control of Hardware Assets" and "Control 2: Inventory and Control of Software Assets"

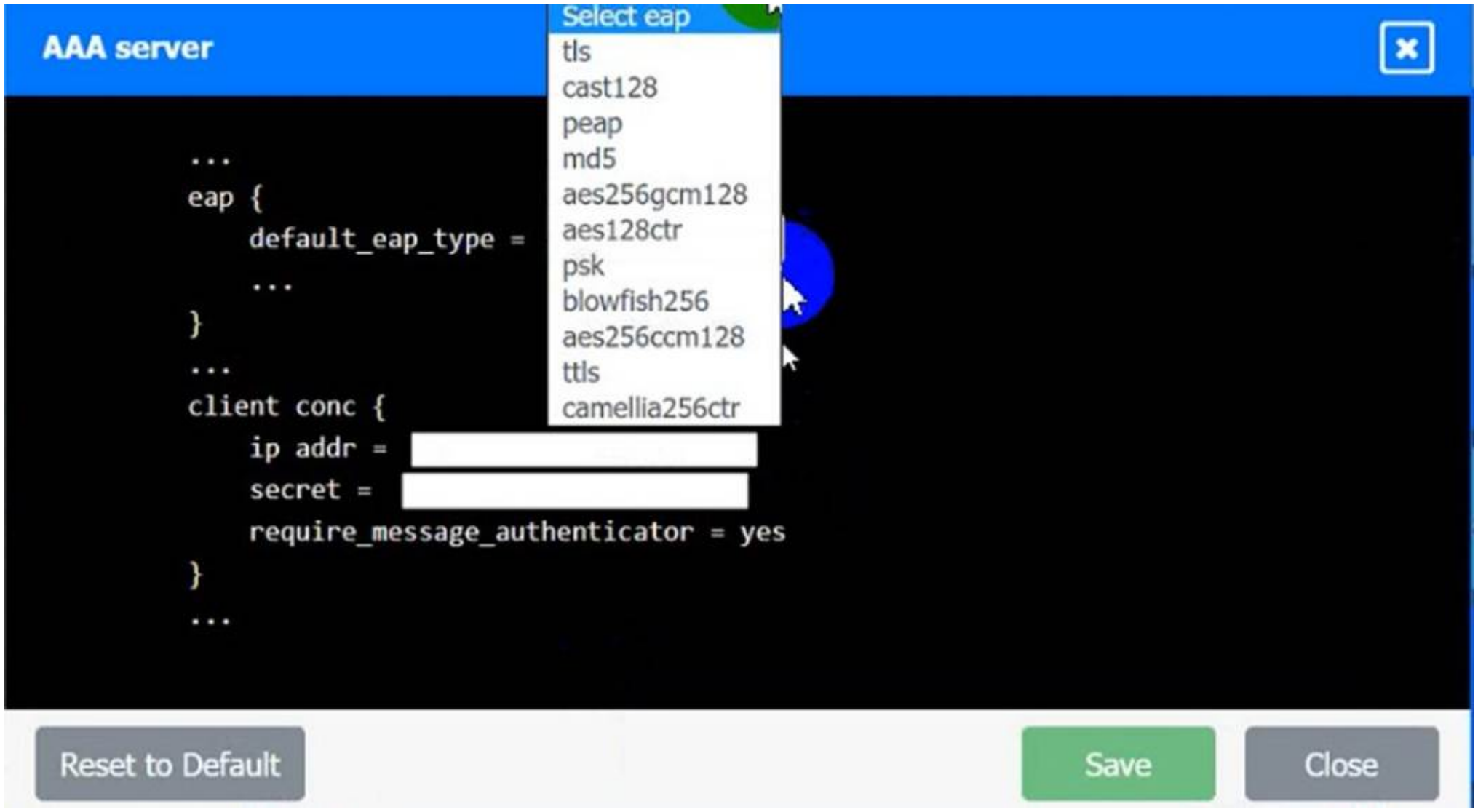
NEW QUESTION 57
SIMULATION
An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.
Complete the configuration files to meet the following requirements:
• The EAP method must use mutual certificate-based authentication (With 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:



AAA Server:

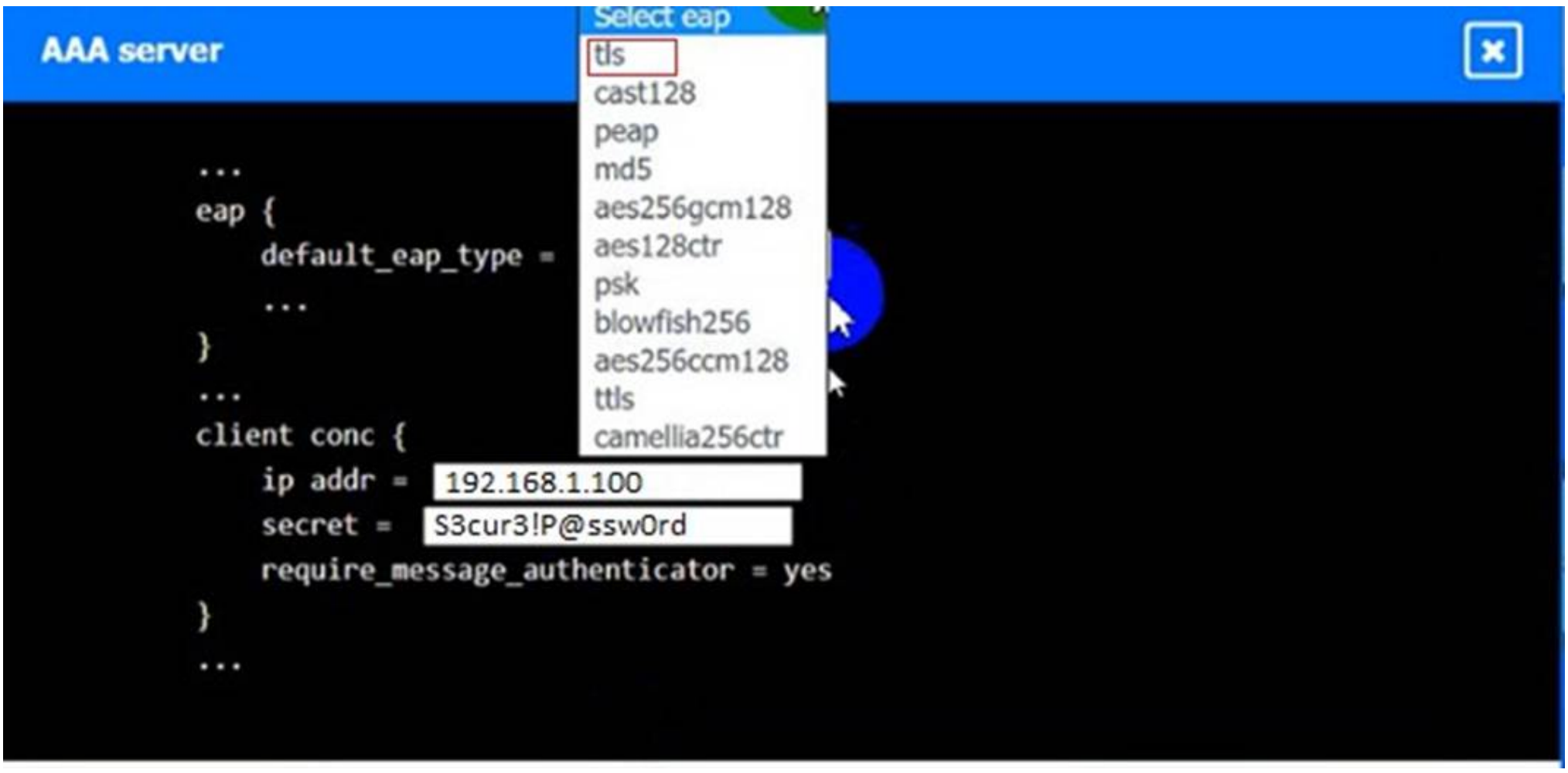


A. Mastered
B. Not Mastered

Answer: A

Explanation:
VPN Concentrator:

AAA Server:



NEW QUESTION 59
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 laC 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 63
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 com 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 LOAP Which of the following is me b»« way to reduce the risk oi reoccurrence?

A. Enforcing allow lists for authorized network pons and protocols
B. Measuring and attesting to the entire boot chum
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

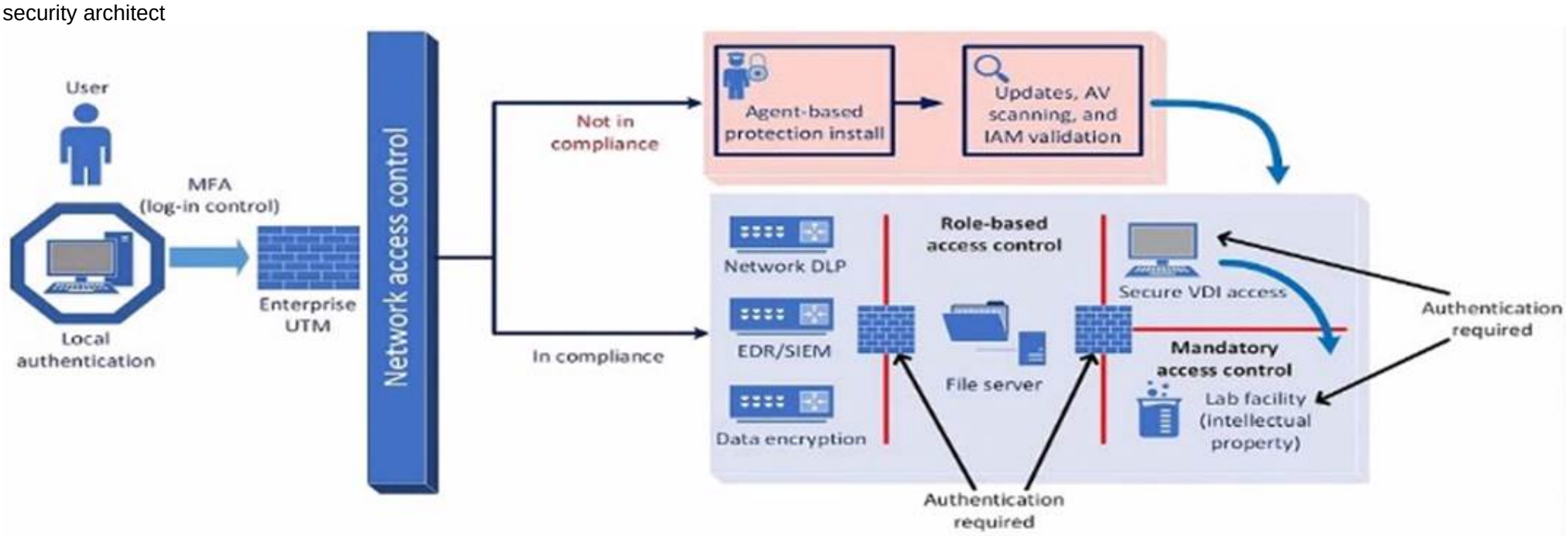
NEW QUESTION 67
An organization is required to
* Respond to internal and external inquiries in a timely manner
* Provide transparency.
* Comply with regulatory requirements
The organization has not experienced any reportable breaches but wants to be prepared if a breach occurs in the future. Which of the following is the best way for the organization to prepare?

A. Outsourcing the handling of necessary regulatory filing to an external consultant
B. Integrating automated response mechanisms into the data subject access request process
C. Developing communication templates that have been vetted by internal and external counsel
D. Conducting lessons-learned activities and integrating observations into the crisis management plan

Answer: C

Explanation:
Preparing communication templates that have been vetted by both internal and external counsel ensures that the organization can respond quickly and effectively to internal and external inquiries, comply with regulatory requirements, and provide transparency in the event of a breach.
Why Communication Templates?
? Timely Response: Pre-prepared templates ensure that responses are ready to be deployed quickly, reducing response time.
? Regulatory Compliance: Templates vetted by counsel ensure that all communications meet legal and regulatory requirements.
? Consistent Messaging: Ensures that all responses are consistent, clear, and
accurate, maintaining the organization??s credibility.
? Crisis Management: Pre-prepared templates are a critical component of a broader crisis management plan, ensuring that all stakeholders are informed appropriately.
Other options, while useful, do not provide the same level of preparedness and compliance:
? A. Outsourcing to an external consultant: This may delay response times and lose
internal control over the communication.
? B. Integrating automated response mechanisms: Useful for efficiency but not for ensuring compliant and vetted responses.
? D. Conducting lessons-learned activities: Important for improving processes but does not provide immediate preparedness for communication.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"
? ISO/IEC 27002:2013, "Information technology — Security techniques — Code of practice for information security controls"

NEW QUESTION 69
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 74
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 tor 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 76
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 77
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 82
A security analyst is reviewing the following event timeline from an COR solution:

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

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

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

Answer: C

Explanation:
The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed. This suggests a Time-Of- Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.
References:
? CompTIA SecurityX Study Guide: Discusses TOCTOU vulnerabilities as a timing attack where the state of a resource changes after it has been validated.
? NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations": Recommends addressing TOCTOU vulnerabilities to ensure the integrity of security operations.
? "The Art of Software Security Assessment" by Mark Dowd, John McDonald, and Justin Schuh: Covers logic flaws and timing vulnerabilities, including TOCTOU issues.

NEW QUESTION 84
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	10.123.34.90	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	10.60.65.11	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 87
An incident response team is analyzing malware and observes the following:
• Does not execute in a sandbox
• No network loCs
• 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 91
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 nave 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 96
A security administrator needs to automate alerting. The server generates structured log files that need to be parsed to determine whether an alarm has been triggered Given the following code function:

```
def parse_logs(logfile):
    with open(logfile) as log_file:
        parsed_log = json.load(log_file)
    if parsed_log["error_log"]["system_1"]["InAlarmState"]:
```

Which of the following is most likely the log input that the code will parse?
A)

```
["error_log]
    ["system_1"]
        ["InAlarmState": True]
```

B)

```
<"error_log"><"system_1"></"InAlarmState"="True"></"system_1"></"error_log">
```

C)

```
error_log:
    - system_1:
      InAlarmState: True
```

D)

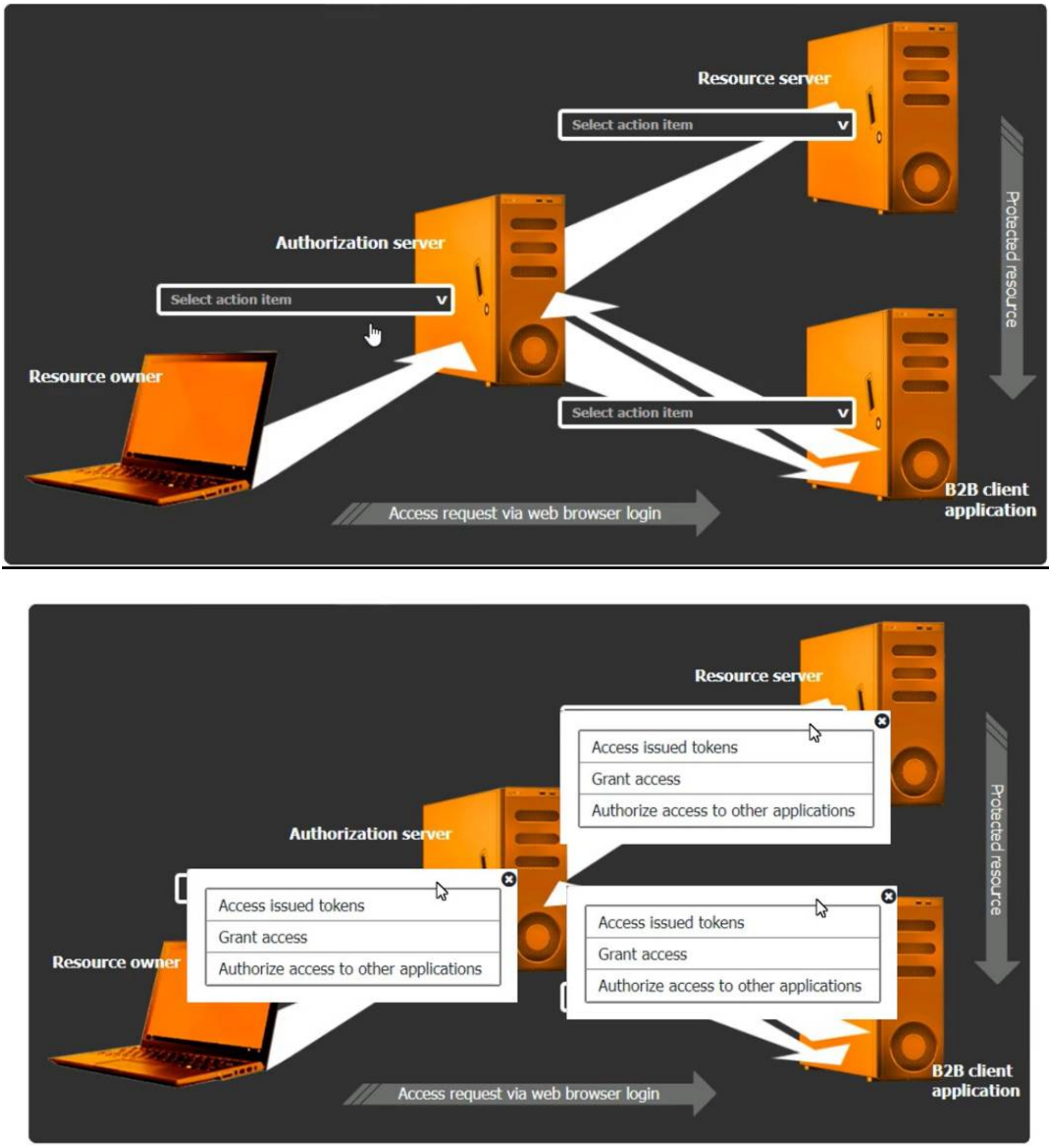
```
{"error_log": {"system_1": {"InAlarmState": True }}}
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:
The code function provided in the question seems to be designed to parse JSON formatted logs to check for an alarm state. Option A is a JSON format that matches the structure likely expected by the code. The presence of the "error_log" and "InAlarmState" keys suggests that this is the correct input format.
Reference: CompTIA SecurityX Study Guide, Chapter on Log Management and Automation, Section on Parsing Structured Logs.

NEW QUESTION 99
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 104
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 108
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 112

Asecuntv administrator is performing a gap assessment against a specific OS benchmark The benchmark requires the following configurations be applied to endpomts:
• 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 114
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 117
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 118
The material finding from a recent compliance audit indicate a company has an issue with excessive permissions. The findings show that employees changing roles or departments results in privilege creep. Which of the following solutions are the best ways to mitigate this issue? (Select two).
Setting different access controls defined by business area

A. Implementing a role-based access policy
B. Designing a least-needed privilege policy
C. Establishing a mandatory vacation policy
D. Performing periodic access reviews
E. Requiring periodic job rotation

Answer: AD

Explanation:
To mitigate the issue of excessive permissions and privilege creep, the best solutions are:
? Implementing a Role-Based Access Policy:
? Performing Periodic Access Reviews:

NEW QUESTION 121
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 125
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 > /ete/passwd
B. Installing an EDR on the container's host with reporting configured to log to a centralized SIFM and Implementing the followingalerting rules TF PBOCESS_USEB=rooC ALERT_TYPE=critical
C. Designing a muiticontainer 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 networ
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 126

A security analyst wants to use lessons learned from a poor incident response to reduce dwell lime in the future The analyst is using the following data points

User	Site visited	HTTP method	Filter status	Traffic status	Alert status
account1	tools.com	GET	Allowed	Allowed	No
admin1	hacking.com	GET	Allowed	Allowed	Yes
account5	payroll.com	GET	Allowed	Allowed	No
account2	p4yr0ll.com	GET	Blocked	Blocked	No
account2	p4yr0ll.com	POST	Blocked	Blocked	No
account2	139.40.29.21	POST	Allowed	Allowed	No
account5	payroll.com	GET	Allowed	Allowed	No

Which of the following would the analyst most likely recommend?

A. Adjusting the SIEM to alert on attempts to visit phishing sites
B. Allowing TRACE method traffic to enable better log correlation
C. Enabling alerting on all suspicious administrator behavior
D. utilizing allow lists on the WAF for all users using GFT methods

Answer: C

Explanation:
In the context of improving incident response and reducing dwell time, the security analyst needs to focus on proactive measures that can quickly detect and alert on potential security breaches. Here??s a detailed analysis of the options provided:
* A. Adjusting the SIEM to alert on attempts to visit phishing sites: While this is a useful measure to prevent phishing attacks, it primarily addresses external threats and doesn??t directly impact dwell time reduction, which focuses on the time a threat remains undetected within a network.
* B. Allowing TRACE method traffic to enable better log correlation: The TRACE method in HTTP is used for debugging purposes, but enabling it can introduce security vulnerabilities. It??s not typically recommended for enhancing security monitoring or incident response.
* C. Enabling alerting on all suspicious administrator behavior: This option directly targets the potential misuse of administrator accounts, which are often high-value targets for attackers. By monitoring and alerting on suspicious activities from admin accounts, the organization can quickly identify and respond to potential breaches, thereby reducing dwell
time significantly. Suspicious behavior could include unusual login times, access to sensitive data not usually accessed by the admin, or any deviation from normal behavior patterns. This proactive monitoring is crucial for quick detection and response, aligning well with best practices in incident response.
* D. Utilizing allow lists on the WAF for all users using GET methods: This measure is aimed at restricting access based on allowed lists, which can be effective in preventing unauthorized access but doesn??t specifically address the need for quick detection and response to internal threats.
References:
? CompTIA SecurityX Study Guide: Emphasizes the importance of monitoring and alerting on admin activities as part of a robust incident response plan.
? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide": Highlights best practices for incident response, including the importance of detecting and responding to suspicious activities quickly.
? "Incident Response & Computer Forensics" by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia: Discusses techniques for reducing dwell time through effective monitoring and alerting mechanisms, particularly focusing on privileged account activities.
By focusing on enabling alerting for suspicious administrator behavior, the security analyst addresses a critical area that can help reduce the time a threat goes undetected, thereby improving the overall security posture of the organization.
Top of Form Bottom of Form

NEW QUESTION 128
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 131
A senior security engineer flags me following log file snippet as hawing 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 10.80.9.3
-------------| fshare A 10.80.9.4
-------------| sip A 10.80.9.5
-------------| msn-crit-apps A 10.81.22.33
...
```

Which of the following solutions, if implemented, would mitigate the nsk of this issue reoccurnnp?
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 136
An organization is developing on Al-enabled digital worker to help employees complete common tasks such as template development, editing, research, and scheduling. As part of the Al workload the organization wants to Implement guardrails within the platform. Which of the following should the company do to secure the Al environment?

A. Limn 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 138
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 142
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 1AM 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 145
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 147
While reviewing recent modem reports, a security officer discovers that several employees were contacted by the same individual who impersonated a recruiter. Which of the following best describes this type of correlation?

A. Spear-phishing campaign
B. Threat modeling
C. Red team assessment
D. Attack pattern analysis

Answer: A

Explanation:
The situation where several employees were contacted by the same individual impersonating a recruiter best describes a spear-phishing campaign. Here??s why:
? Targeted Approach: Spear-phishing involves targeting specific individuals within an organization with personalized and convincing messages to trick them into divulging sensitive information or performing actions that compromise security.
? Impersonation: The use of impersonation, in this case, a recruiter, is a common tactic in spear-phishing to gain the trust of the targeted individuals and increase the likelihood of a successful attack.
? Correlated Contacts: The fact that several employees were contacted by the same individual suggests a coordinated effort to breach the organization??s security by targeting multiple points of entry through social engineering.
? References:

NEW QUESTION 150
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
```

Analysis: Select analysis

- 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.

Remediation: Select 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 blocklist for known malicious ports.
- No further action is needed.

IoC 1 | IoC 2 | IoC 3

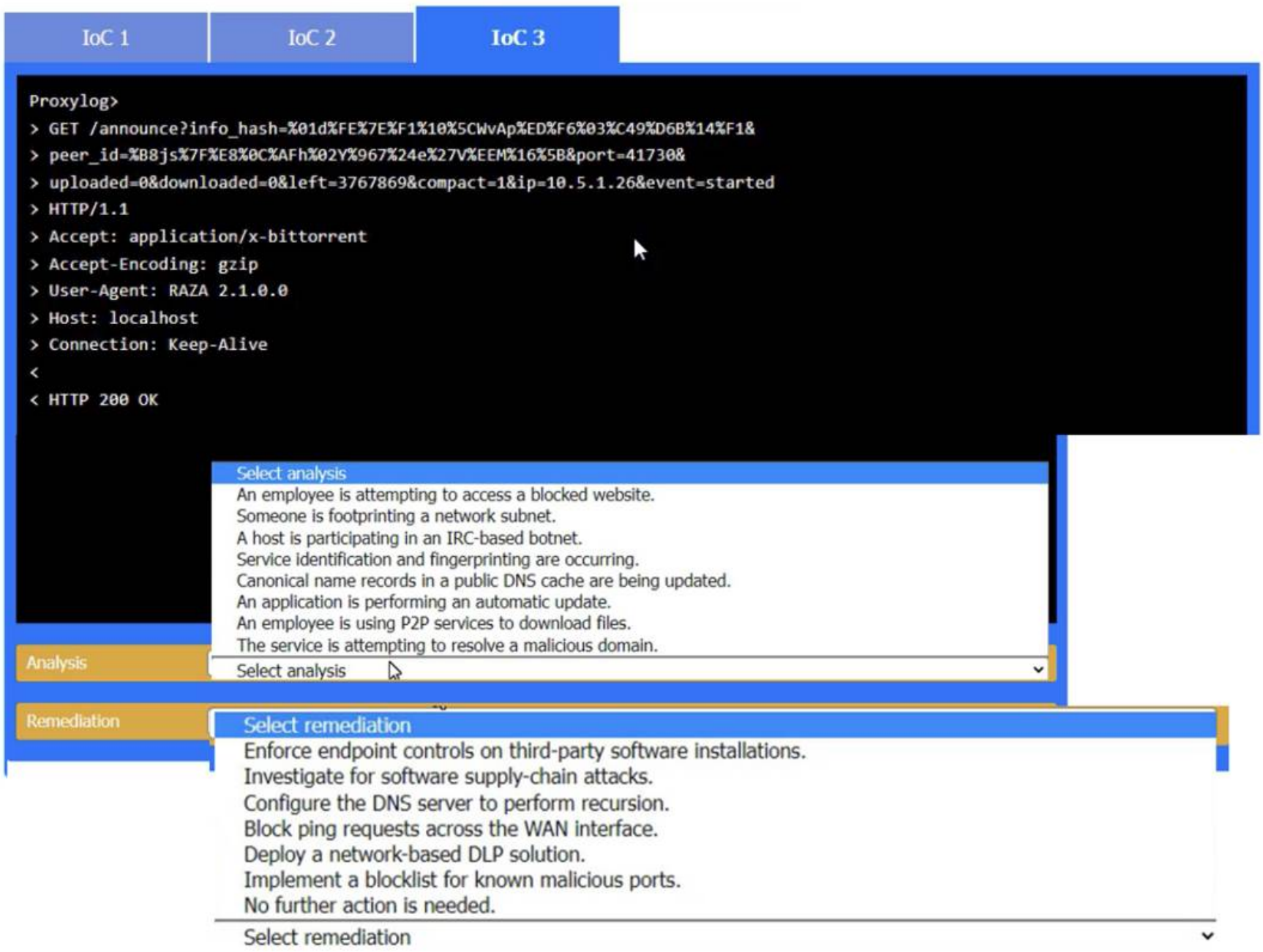
```
Src        Dst        Proto     Data   Action
10.0.5.5   10.1.2.1   IP_ICMP   ECHO   Drop
10.0.5.5   10.1.2.2   IP_ICMP   ECHO   Drop
10.0.5.5   10.1.2.3   IP_ICMP   ECHO   Drop
10.0.5.5   10.1.2.4   IP_ICMP   ECHO   Drop
10.0.5.5   10.1.2.5   IP_ICMP   ECHO   Drop
```

Analysis: Select analysis

- 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.

Remediation: Select 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 blocklist for known malicious ports.
- No further action is needed.



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 154
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 155
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

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