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
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 3
After some employees were caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation. Which of the following would the company most likely do to decrease this type of risk?

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

Answer: B

Explanation:
A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Implementing a CASB provides several benefits:
? A. Improve firewall rules to avoid access to those platforms: This can help but is not as effective or comprehensive as a CASB.
? B. Implement a cloud-access security broker: A CASB can provide visibility into cloud application usage, enforce data security policies, and protect against data

leaks by monitoring and controlling access to cloud services. It also provides advanced features like data encryption, data loss prevention (DLP), and compliance monitoring.
? C. Create SIEM rules to raise alerts for access to those platforms: This helps in
monitoring but does not prevent data leaks.
? D. Deploy an internet proxy that filters certain domains: This can block access to specific sites but lacks the granular control and visibility provided by a CASB.
Implementing a CASB is the most comprehensive solution to decrease the risk of data leaks by providing visibility, control, and enforcement of security policies for cloud services. References:
? CompTIA Security+ Study Guide
? Gartner, "Magic Quadrant for Cloud Access Security Brokers"
? NIST SP 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"

NEW QUESTION 4
A security analyst discovered requests associated with IP addresses known for born legitimate 3nd bot-related traffic. Which of the following should the analyst use to determine whether the requests are malicious?

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

Answer: A

Explanation:
The user-agent string can provide valuable information to distinguish between legitimate and bot-related traffic. It contains details about the browser, device, and sometimes the operating system of the client making the request.
Why Use User-Agent String?
? Identify Patterns: User-agent strings can help identify patterns that are typical of bots or legitimate users.
? Block Malicious Bots: Many bots use known user-agent strings, and identifying these can help block malicious requests.
? Anomalies Detection: Anomalous user-agent strings can indicate spoofing attempts or malicious activity.
Other options provide useful information but may not be as effective for initial determination of the nature of the request:
? B. Byte length of the request: This can indicate anomalies but does not provide
detailed information about the client.
? C. Web application headers: While useful, they may not provide enough distinction between legitimate and bot traffic.
? D. HTML encoding field: This is not typically used for identifying the nature of the request.
References:
? CompTIA SecurityX Study Guide
? "User-Agent Analysis for Security," OWASP
? NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)"

NEW QUESTION 5
Users are willing passwords on paper because of the number of passwords needed in an environment. Which of the following solutions is the best way to manage this situation and decrease risks?

A. Increasing password complexity to require 31 least 16 characters
B. implementing an SSO solution and integrating with applications
C. Requiring users to use an open-source password manager
D. Implementing an MFA solution to avoid reliance only on passwords

Answer: B

Explanation:
Implementing a Single Sign-On (SSO) solution and integrating it with applications is the best way to manage the situation and decrease risks. Here??s why:
? Reduced Password Fatigue: SSO allows users to log in once and gain access to multiple applications and systems without needing to remember and manage multiple passwords. This reduces the likelihood of users writing down passwords.
? Improved Security: By reducing the number of passwords users need to manage, SSO decreases the attack surface and potential for password-related security breaches. It also allows for the implementation of stronger authentication methods.
? User Convenience: SSO improves the user experience by simplifying the login process, which can lead to higher productivity and satisfaction.
? References:

NEW QUESTION 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 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 8
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 9
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 10
Which of the following is the main reason quantum computing advancements are leading companies and countries to deploy new encryption algorithms?

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

Answer: A

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

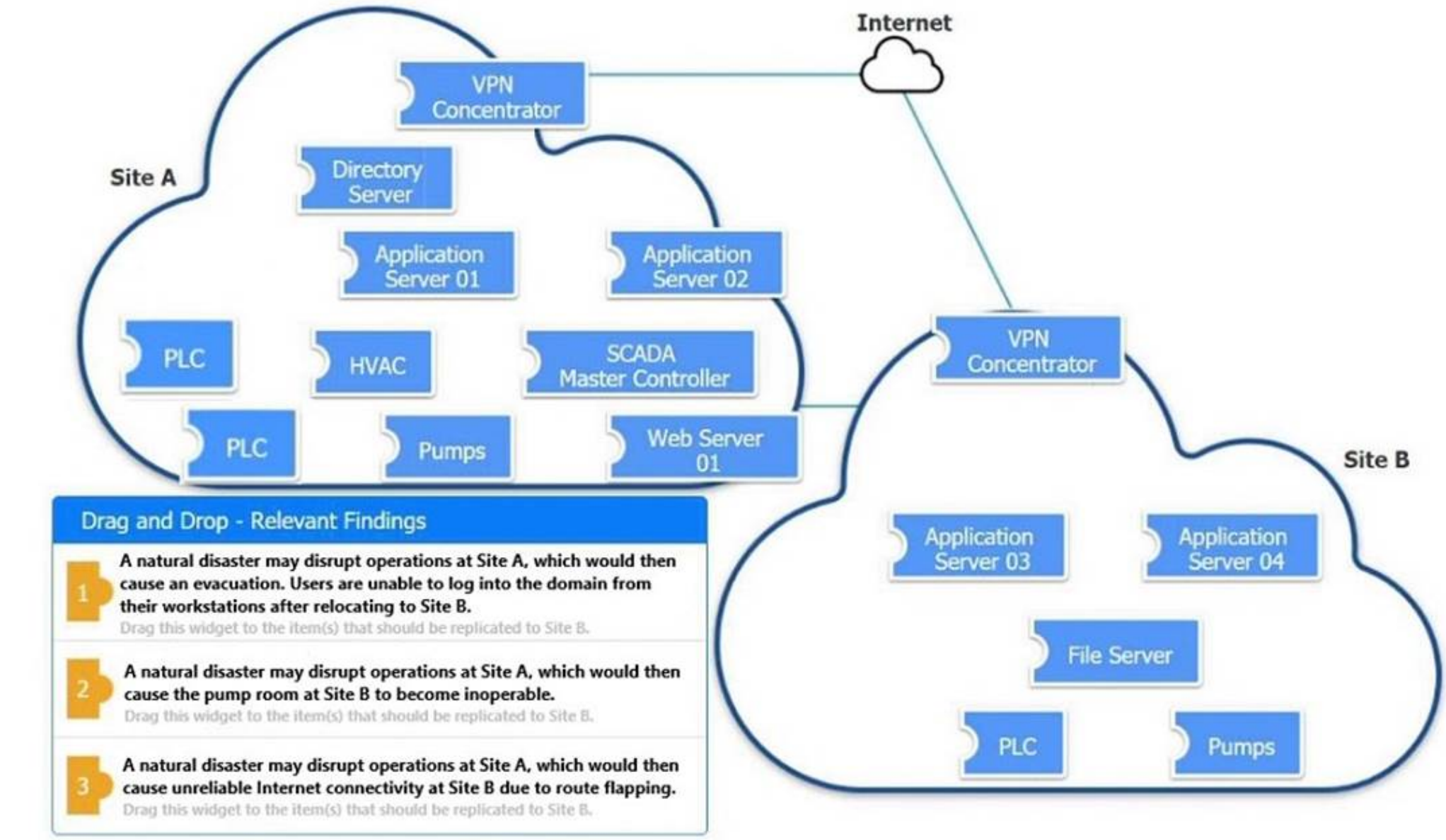
NEW QUESTION 10
A security officer received several complaints from users about excessive MPA push notifications at night The security team investigates and suspects malicious activities regarding user account authentication Which of the following is the best way for the security officer to restrict 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

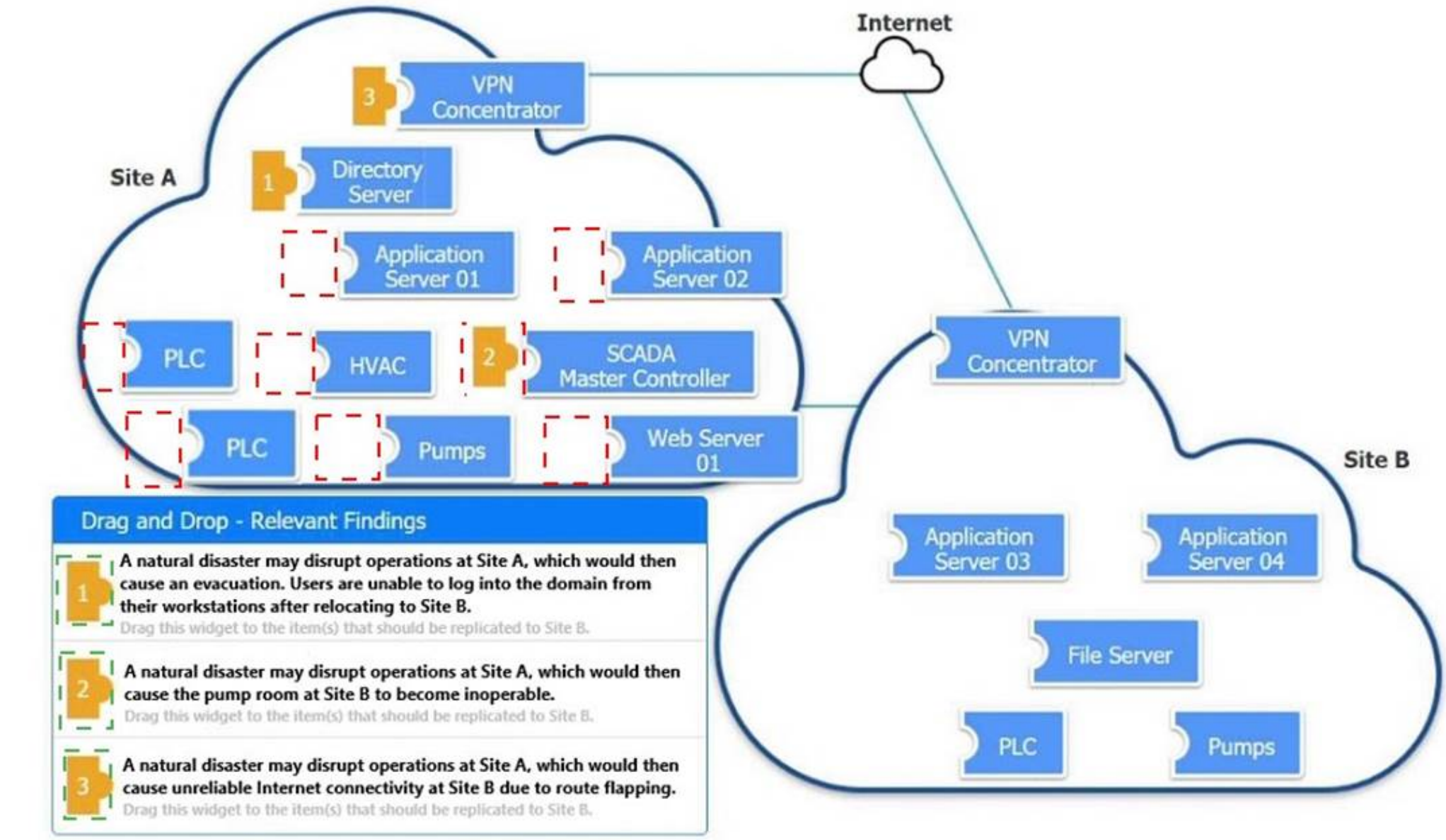
Answer: D

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 12
DRAG DROP
An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS



Review the following scenarios and instructions. Match each relevant finding to the affected host.
After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.
Each finding may be used more than once.
If at any time you would like to bring back the initial state of the simul-ation, please click the Reset All button.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 13
A security engineer is developing a solution to meet the following requirements?
• All endpoints should be able to establish telemetry with a SIEM.
• All endpoints should be able to be integrated into the XDR platform.
• SOC services should be able to monitor the XDR platform
Which of the following should the security engineer implement to meet the requirements?

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

Answer: D

Explanation:
To meet the requirements of having all endpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR platform, the best approach is to implement Host Intrusion Prevention Systems (HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host- based firewall ensures that only authorized traffic is allowed, providing an additional layer of security.
References:
? CompTIA SecurityX Study Guide: Describes the roles of HIPS and host-based firewalls in endpoint security and their integration with SIEM and XDR platforms.
? NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)": Highlights the capabilities of HIPS for security monitoring and incident response.
? "Network Security Monitoring" by Richard Bejtlich: Discusses the integration of various security tools, including HIPS and firewalls, for effective security monitoring.

NEW QUESTION 16
A security configure is building a solution to disable weak CBC configuration for remote access connections lo Linux systems. Which of the following should the security engineer modify?

A. The /etc/openssl.conf file, updating the virtual site parameter
B. The /etc/nsswith.conf file, updating the name server
C. The /etc/hosts file, updating the IP parameter
D. The /etc/etc/sshd, configure file updating the ciphers

Answer: D

Explanation:
The sshd_config file is the main configuration file for the OpenSSH server. To disable weak CBC (Cipher Block Chaining) ciphers for SSH connections, the security engineer should modify the sshd_config file to update the list of allowed ciphers. This file typically contains settings for the SSH daemon, including which encryption algorithms are allowed.
By editing the /etc/ssh/sshd_config file and updating the Ciphers directive, weak ciphers can be removed, and only strong ciphers can be allowed. This change ensures that the
SSH server does not use insecure encryption methods.
References:
? CompTIA Security+ Study Guide
? OpenSSH manual pages (man sshd_config)
? CIS Benchmarks for Linux

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

Date	Time	Computer	Account	Log-in success?
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM08	User8	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM12	User12	Yes
12/15	8:01:23AM	VM01	User1	Yes
12/15	8:01:23AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:25AM	VM01	User2	No
12/15	8:01:25AM	VM08	User8	Yes

Which of the following should the analyst do first?

A. Disable User2's account
B. Disable User12's account
C. Disable User8's account
D. Disable User1's account

Answer: D

Explanation:
Based on the provided authentication logs, we observe that User1's account experienced multiple failed login attempts within a very short time span (at 8:01:23 AM on 12/15). This pattern indicates a potential brute-force attack or an attempt to gain unauthorized access. Here??s a breakdown of why disabling User1's account is the appropriate first step:
? Failed Login Attempts: The logs show that User1 had four consecutive failed login attempts:
? Security Protocols and Best Practices: According to CompTIA Security+ guidelines, multiple failed login attempts within a short timeframe should trigger an immediate response to prevent further potential unauthorized access attempts. This typically involves temporarily disabling the account to stop ongoing brute-force attacks.
? Account Lockout Policy: Implementing an account lockout policy is a standard practice to thwart brute-force attacks. Disabling User1's account will align with these best practices and prevent further failed attempts, which might lead to successful unauthorized access if not addressed.
? References:
By addressing User1's account first, we effectively mitigate the immediate threat of a brute- force attack, ensuring that further investigation can be conducted without the risk of unauthorized access continuing during the investigation period.

NEW QUESTION 26
Which of the following is the security engineer most likely doing?

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

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

Answer: A

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

NEW QUESTION 30
A company receives several complaints from customers regarding its website. An engineer implements a parser for the web server logs that generates the following output:

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

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

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

Answer: B

Explanation:
The table indicates varying load times for users accessing the website from different geographic locations. Customers from Australia and India are experiencing significantly higher load times compared to those from the United States. This suggests that latency and geographical distance are affecting the website's performance.
? A. IDS (Intrusion Detection System): While an IDS is useful for detecting malicious
activities, it does not address performance issues related to latency and geographical distribution of content.
? B. CDN (Content Delivery Network): A CDN stores copies of the website's content
in multiple geographic locations. By serving content from the nearest server to the user, a CDN can significantly reduce load times and improve user experience globally.
? C. WAF (Web Application Firewall): A WAF protects web applications by filtering and monitoring HTTP traffic but does not improve performance related to geographical latency.
? D. NAC (Network Access Control): NAC solutions control access to network
resources but are not designed to address web performance issues.
Implementing a CDN is the best solution to resolve the performance issues observed in the log output.
References:
? CompTIA Security+ Study Guide
? "CDN: Content Delivery Networks Explained" by Akamai Technologies
? NIST SP 800-44, "Guidelines on Securing Public Web Servers"

NEW QUESTION 35
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 37
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 42
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 44
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 46
An organization mat performs real-time financial processing is implementing a new backup solution Given the following business requirements?
* The backup solution must reduce the risk for potential backup compromise

* The backup solution must be resilient to a ransomware attack.
* The time to restore from backups is less important than the backup data integrity
* Multiple copies of production data must be maintained
Which of the following backup strategies best meets these requirement?

A. Creating a secondary, immutable storage array and updating it with live data on a continuous basis
B. Utilizing two connected storage arrays and ensuring the arrays constantly sync
C. Enabling remote journaling on the databases to ensure real-time transactions are mirrored
D. Setting up antitempering on the databases to ensure data cannot be changed unintentionally

Answer: A

Explanation:
? A. Creating a secondary, immutable storage array and updating it with live data on a continuous basis: An immutable storage array ensures that data, once written, cannot be altered or deleted. This greatly reduces the risk of backup compromise
and provides resilience against ransomware attacks, as the ransomware cannot modify or delete the backup data. Maintaining multiple copies of production data with an immutable storage solution ensures data integrity and compliance with the requirement for multiple copies.
Other options:
? B. Utilizing two connected storage arrays and ensuring the arrays constantly sync: While this ensures data redundancy, it does not provide protection against ransomware attacks, as both arrays could be compromised simultaneously.
? C. Enabling remote journaling on the databases: This ensures real-time transaction mirroring but does not address the requirement for reducing the risk of backup compromise or resilience to ransomware.
? D. Setting up anti-tampering on the databases: While this helps ensure data integrity, it does not provide a comprehensive backup solution that meets all the specified requirements.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-209, "Security Guidelines for Storage Infrastructure"
? "Immutable Backup Architecture" by Veeam

NEW QUESTION 47
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 50
Users are experiencing a variety of issues when trying to access corporate resources examples include
• Connectivity issues between local computers and file servers within branch offices
• Inability to download corporate applications on mobile endpoints wtiilc working remotely
• Certificate errors when accessing internal web applications
Which of the following actions are the most relevant when troubleshooting the reported issues? (Select two).

A. Review VPN throughput
B. Check IPS rules
C. Restore static content on lite CDN.
D. Enable secure authentication using NAC
E. Implement advanced WAF rules.
F. Validate MDM asset compliance

Answer: AF

Explanation:
The reported issues suggest problems related to network connectivity, remote access, and certificate management:
? A. Review VPN throughput: Connectivity issues and the inability to download applications while working remotely may be due to VPN bandwidth or performance issues. Reviewing and optimizing VPN throughput can help resolve these problems by ensuring that remote users have adequate bandwidth for accessing corporate resources.
? F. Validate MDM asset compliance: Mobile Device Management (MDM) systems
ensure that mobile endpoints comply with corporate security policies. Validating MDM compliance can help address issues related to the inability to download applications and certificate errors, as non-compliant devices might be blocked from accessing certain resources.
? B. Check IPS rules: While important for security, IPS rules are less likely to directly
address the connectivity and certificate issues described.
? C. Restore static content on the CDN: This action is related to content delivery but does not address VPN or certificate-related issues.
? D. Enable secure authentication using NAC: Network Access Control (NAC) enhances security but does not directly address the specific issues described.

? E. Implement advanced WAF rules: Web Application Firewalls protect web applications but do not address VPN throughput or mobile device compliance.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-77, "Guide to IPsec VPNs"
? CIS Controls, "Control 11: Secure Configuration for Network Devices"

NEW QUESTION 51
A security engineer is given the following requirements:
• An endpoint must only execute Internally signed applications
• Administrator accounts cannot install unauthorized software.
• Attempts to run unauthorized software must be logged Which of the following best meets these requirements?

A. Maintaining appropriate account access through directory management and controls
B. Implementing a CSPM platform to monitor updates being pushed to applications
C. Deploying an EDR solution to monitor and respond to software installation attempts
D. Configuring application control with blocked hashes and enterprise-trusted root certificates

Answer: D

Explanation:
To meet the requirements of only allowing internally signed applications, preventing unauthorized software installations, and logging attempts to run unauthorized software, configuring application control with blocked hashes and enterprise-trusted root certificates is the best solution. This approach ensures that only applications signed by trusted certificates are allowed to execute, while all other attempts are blocked and logged. It effectively prevents unauthorized software installations by restricting execution to pre- approved applications.
References:
? CompTIA SecurityX Study Guide: Describes application control mechanisms and the use of trusted certificates to enforce security policies.
? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations": Recommends application whitelisting and execution control for securing endpoints.
? "The Application Security Handbook" by Mark Dowd, John McDonald, and Justin Schuh: Covers best practices for implementing application control and managing trusted certificates

NEW QUESTION 56
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 61
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

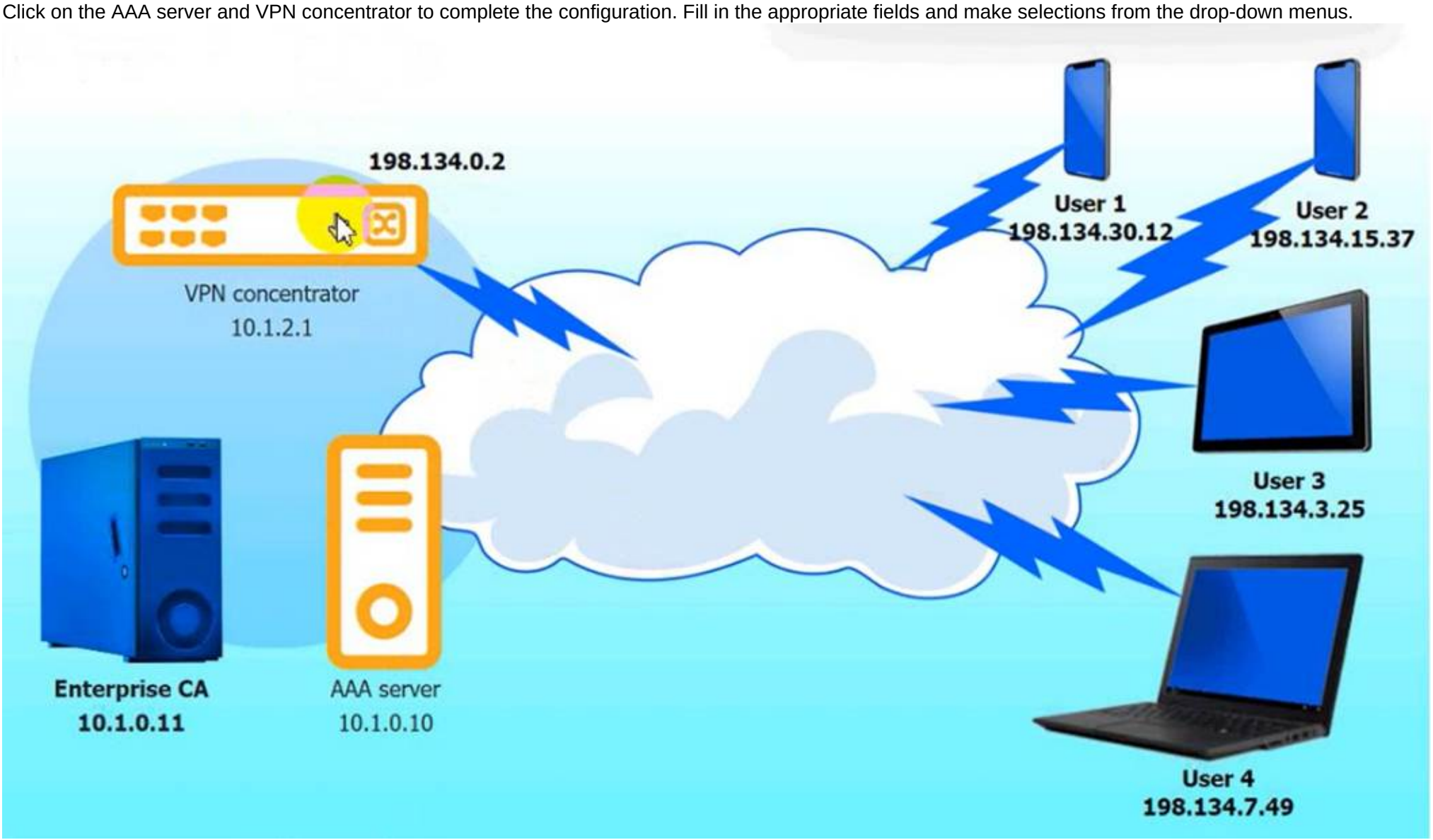
NEW QUESTION 63
A security team is responding to malicious activity and needs to determine the scope of impact the malicious activity appears to affect certain version of an application used by the organization Which of the following actions best enables the team to determine the scope of Impact?

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

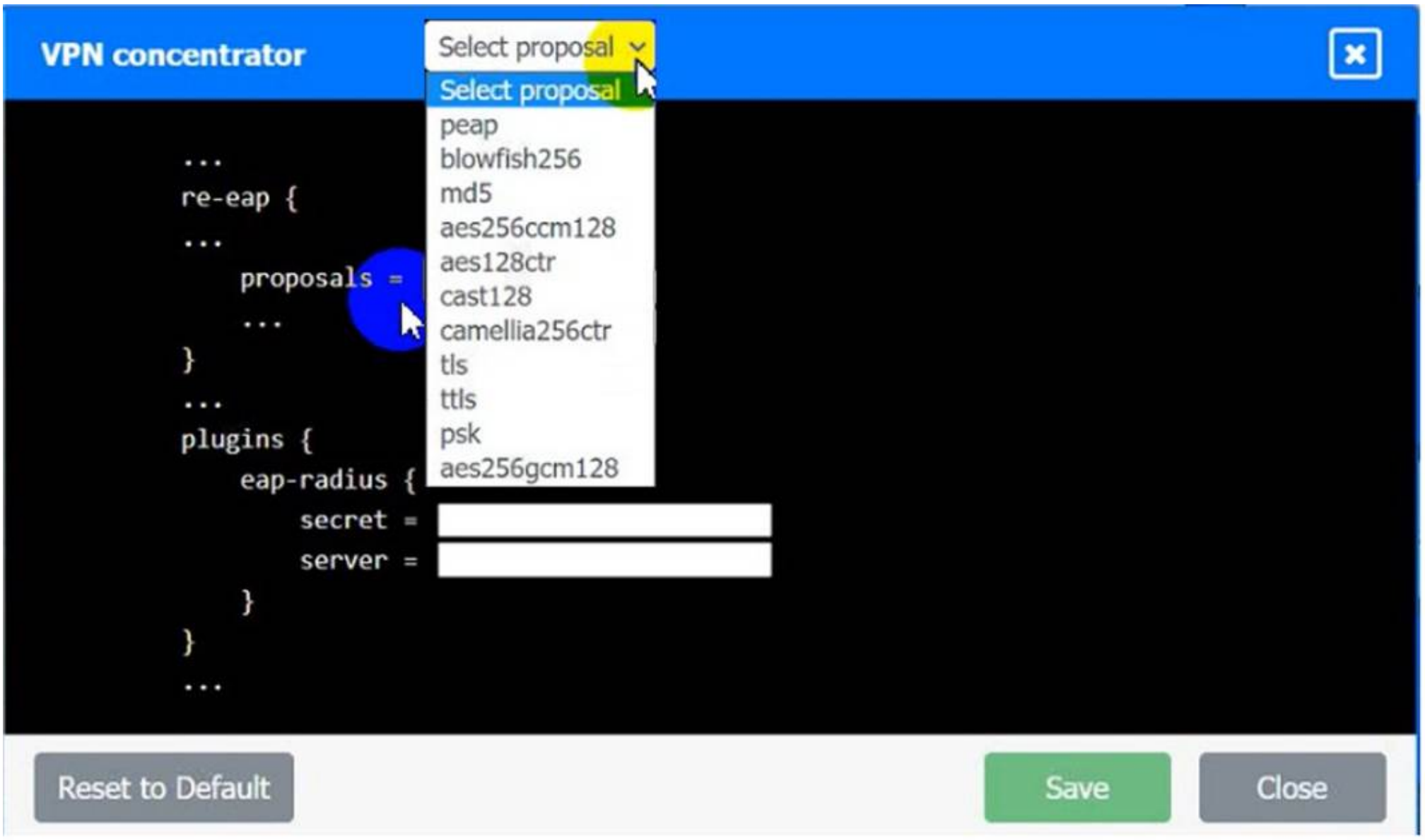
Answer: C

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"

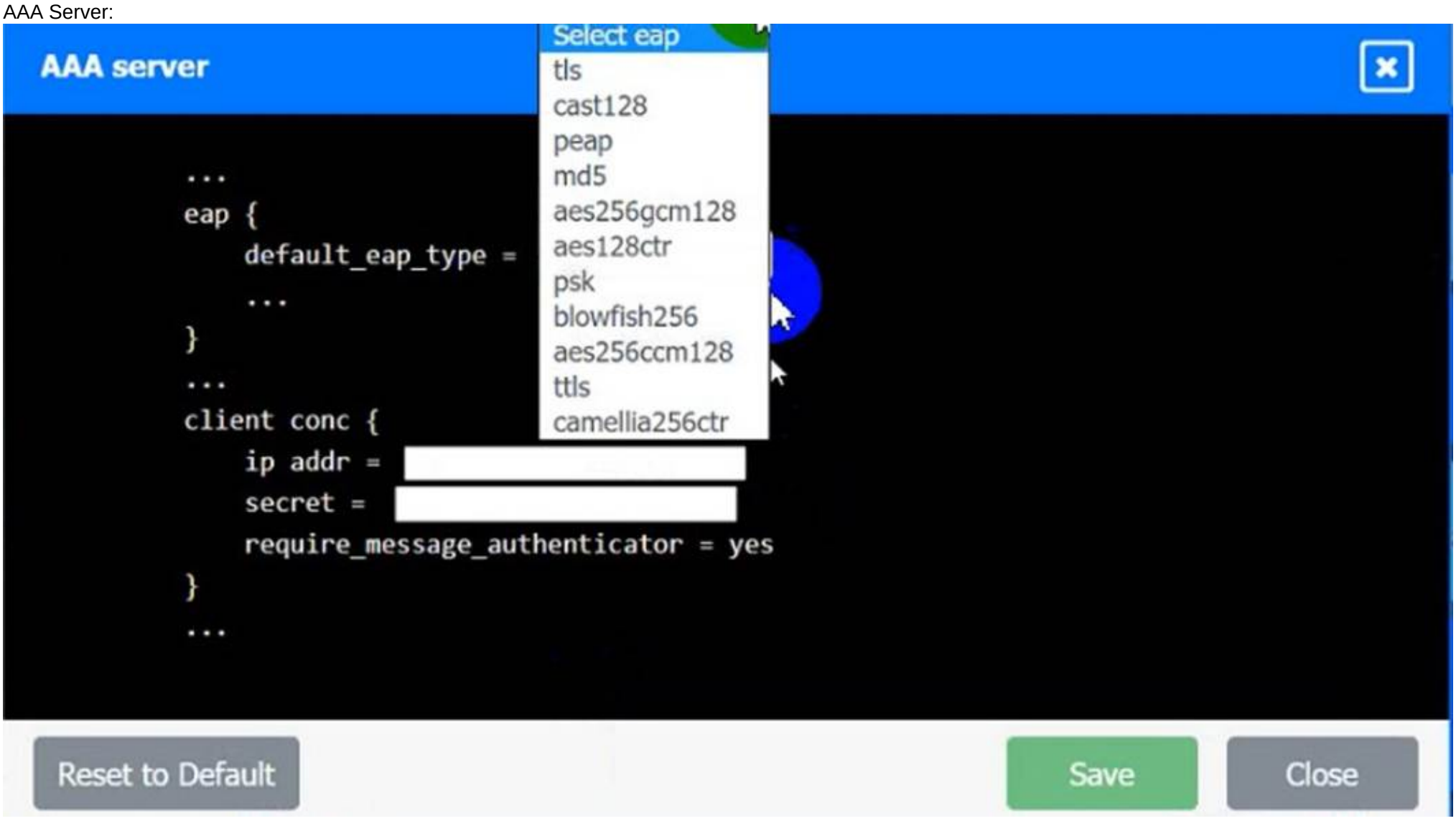
NEW QUESTION 66
SIMULATION
An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.
Complete the configuration files to meet the following requirements:
• The EAP method must use mutual certificate-based authentication (With 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:



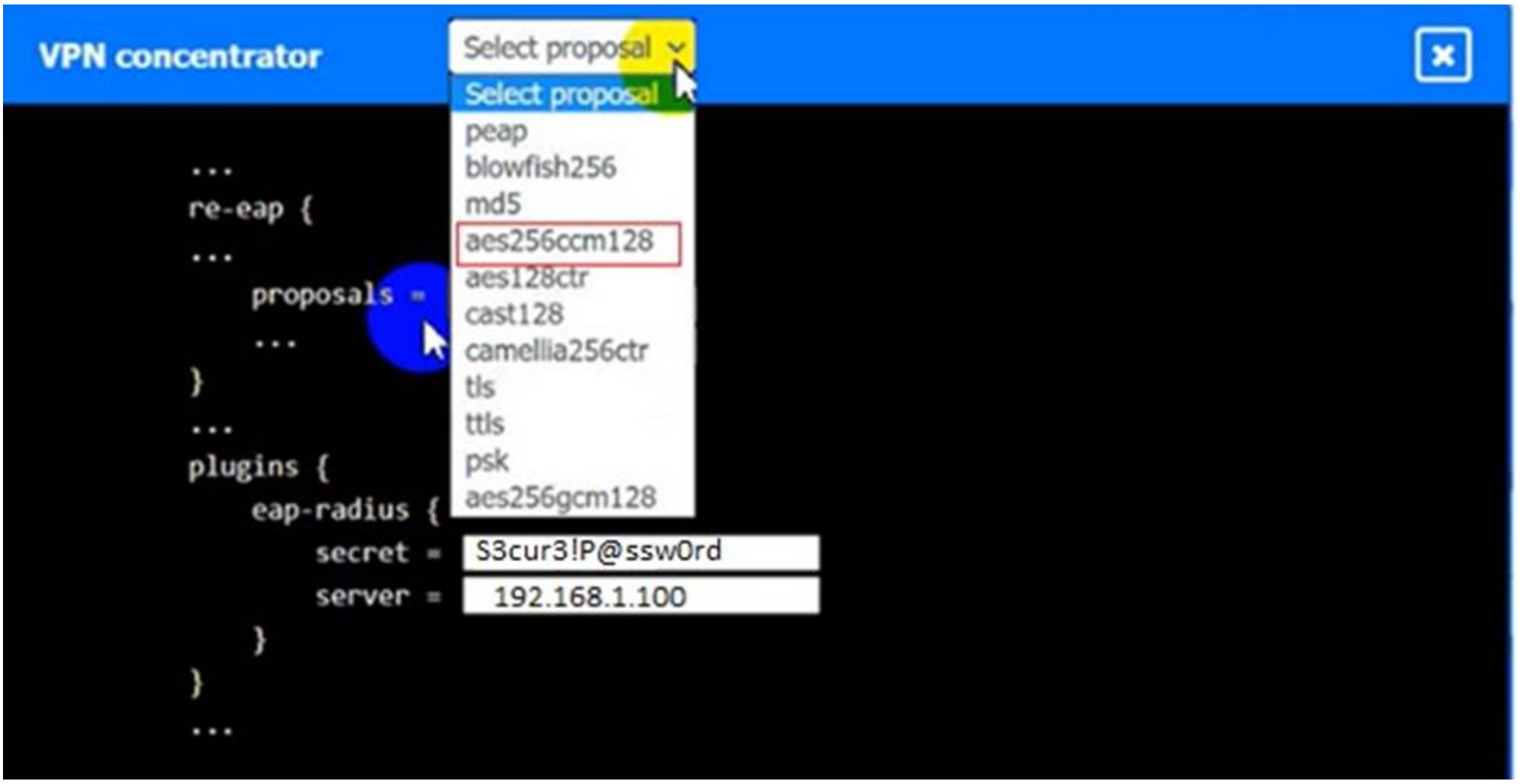
AAA Server:



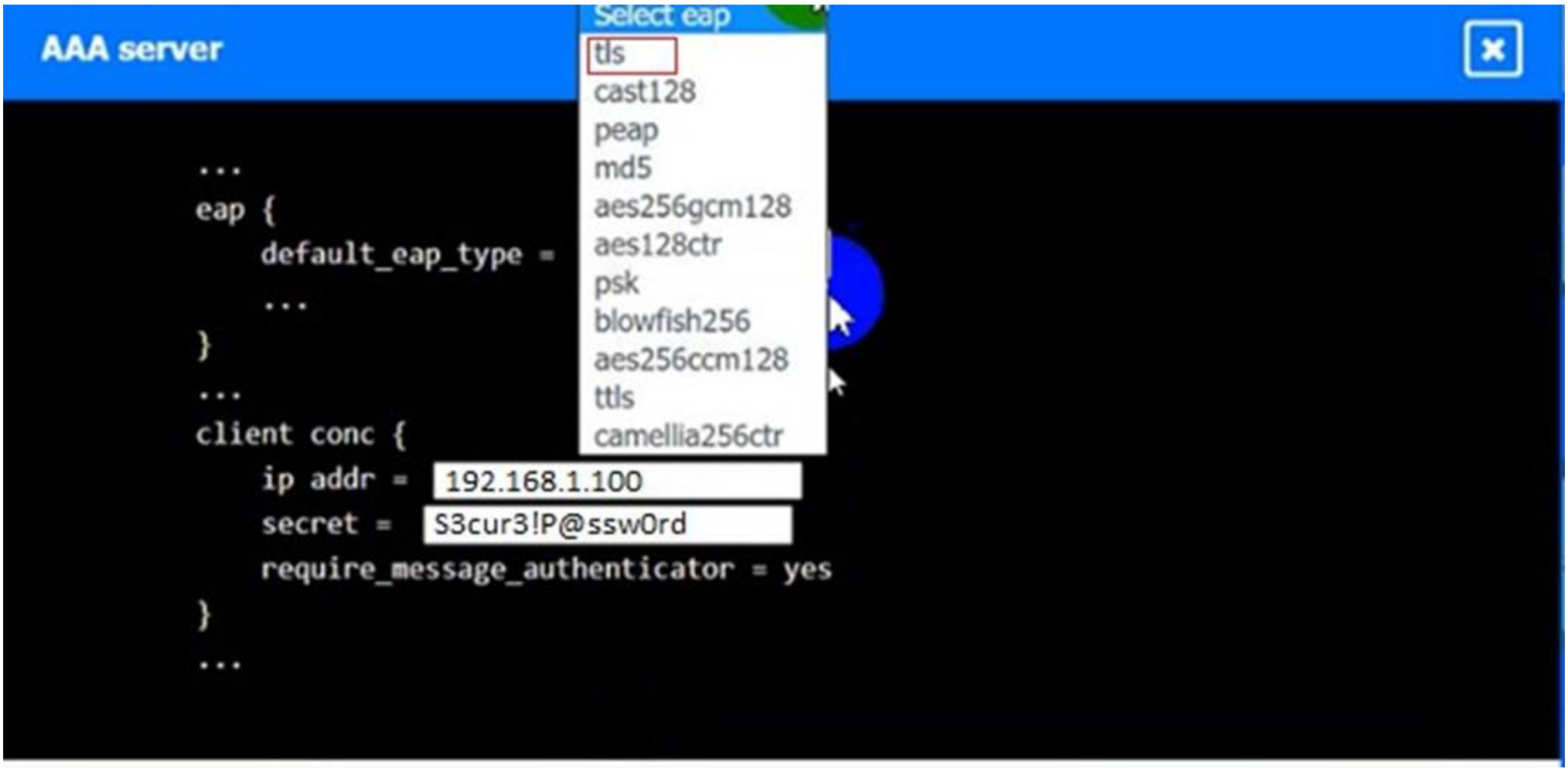
A. Mastered
B. Not Mastered

Answer: A

Explanation:
VPN Concentrator:



AAA Server:



NEW QUESTION 71
A vulnerability can on a web server identified the following:

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

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

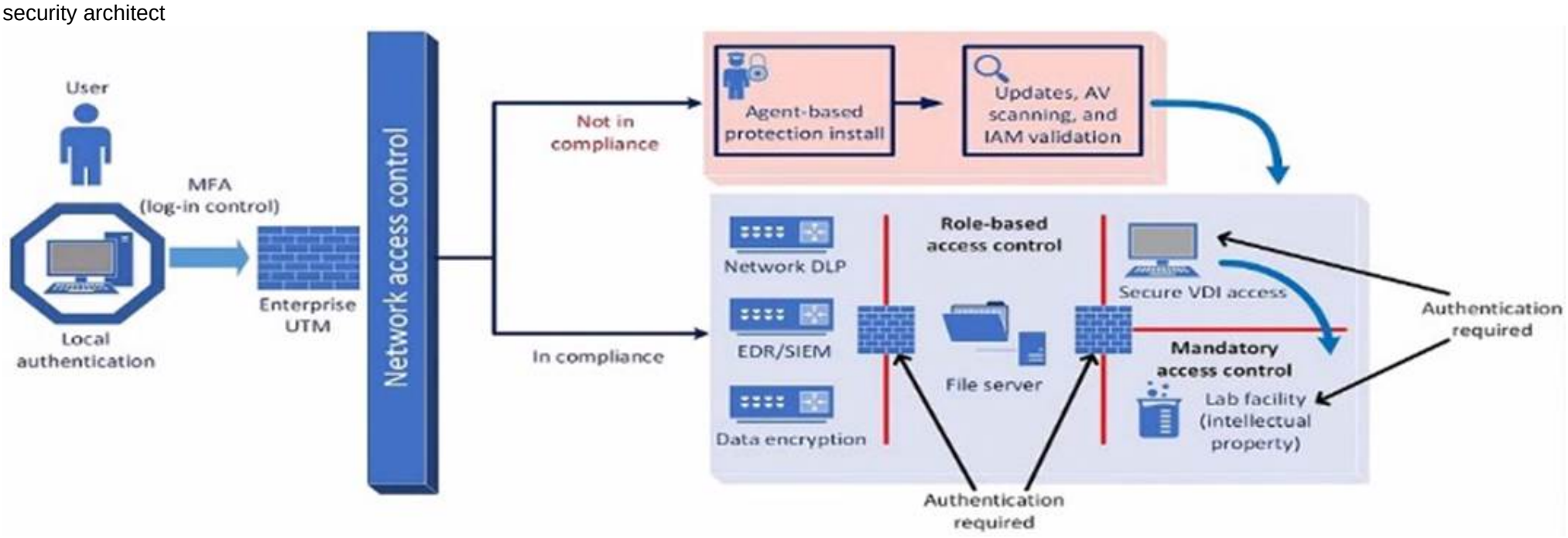
A. Disallowing cipher suites that use ephemeral modes of operation for key agreement
B. Removing support for CBC-based key exchange and signing algorithms
C. Adding TLS_ECDHE_ECDSA_WITH_AE3_256_GCMS_HA256
D. Implementing HIPS rules to identify and block BEAST attack attempts
E. Restricting cipher suites to only allow TLS_RSA_WITH_AES_128_CBC_SHA

F. Increasing the key length to 256 for TLS_RSA_WITH_AES_128_CBC_SHA

Answer: BC

Explanation:
On-path decryption attacks, such as BEAST (Browser Exploit Against SSL/TLS) and other related vulnerabilities, often exploit weaknesses in the implementation of CBC (Cipher Block Chaining) mode. To mitigate these attacks, the following actions are recommended:
? B. Removing support for CBC-based key exchange and signing algorithms: CBC
mode is vulnerable to certain attacks like BEAST. By removing support for CBC- based ciphers, you can eliminate one of the primary vectors for these attacks. Instead, use modern cipher modes like GCM (Galois/Counter Mode) which offer better security properties.
? C. Adding TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256: This cipher
suite uses Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for key exchange, which provides perfect forward secrecy. It also uses AES in GCM mode, which is not susceptible to the same attacks as CBC. SHA-256 is a strong hash function that ensures data integrity.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-52 Rev. 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"
? OWASP (Open Web Application Security Project) guidelines on cryptography and secure communication

NEW QUESTION 74
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 79
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 81
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 82
A security analyst needs to ensure email domains that send phishing attempts without previous communications are not delivered to mailboxes The following email headers are being reviewed

Date	Sending domain	Reply-to domain	Subject
April 16	sales.com	sales-mail.com	Updated Security Questions
April 18	vendor.com	vendor.com	New Sales Catalog
April 18	partner.com	partner.com	B2B Sales Increase
April 19	hr-saas.com	hr-saas.com	Employee Payroll Update Request
April 19	vendor.com	vendor.com	Password Requirements Not Met

Which of the following is the best action for the security analyst to take?

A. Block messages from hr-saas.com because it is not a recognized domain.
B. Reroute all messages with unusual security warning notices to the IT administrator
C. Quarantine all messages with sales-mail.com in the email header
D. Block vendor com for repeated attempts to send suspicious messages

Answer: D

Explanation:
In reviewing email headers and determining actions to mitigate phishing attempts, the security analyst should focus on patterns of suspicious behavior and the reputation of the sending domains. Here??s the analysis of the options provided:
* A. Block messages from hr-saas.com because it is not a recognized domain: Blocking a domain solely because it is not recognized can lead to legitimate emails being missed. Recognition alone should not be the criterion for blocking.
* B. Reroute all messages with unusual security warning notices to the IT administrator: While rerouting suspicious messages can be a good practice, it is not specific to the domain sending repeated suspicious messages.
* C. Quarantine all messages with sales-mail.com in the email header: Quarantining messages based on the presence of a specific domain in the email header can be too broad and may capture legitimate emails.
* D. Block vendor com for repeated attempts to send suspicious messages: This option is the most appropriate because it targets a domain that has shown a pattern of sending suspicious messages. Blocking a domain that repeatedly sends phishing attempts without previous communications helps in preventing future attempts from the same source and aligns with the goal of mitigating phishing risks.
References:
? CompTIA SecurityX Study Guide: Details best practices for handling phishing attempts, including blocking domains with repeated suspicious activity.
? NIST Special Publication 800-45 Version 2, "Guidelines on Electronic Mail Security": Provides guidelines on email security, including the management of suspicious email domains.
? "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft" by Markus Jakobsson and Steven Myers: Discusses effective measures to counter phishing attempts, including blocking persistent offenders.
By blocking the domain that has consistently attempted to send suspicious messages, the security analyst can effectively reduce the risk of phishing attacks.

NEW QUESTION 84
A security analyst Detected unusual network traffic related to program updating processes The analyst collected artifacts from compromised user workstations. The discovered artifacts were binary files with the same name as existing, valid binaries but. with different hashes which of the following solutions would most likely prevent this situation from reoccurring?

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

Answer: B

Explanation:
Implementing digital signatures ensures the integrity and authenticity of software binaries. When a binary is digitally signed, any tampering with the file (e.g., replacing it with a malicious version) would invalidate the signature. This allows systems to verify the origin and integrity of binaries before execution, preventing the execution of unauthorized or compromised binaries.
? A. Improving patching processes: While important, this does not directly address
the issue of verifying the integrity of binaries.
? B. Implementing digital signatures: This ensures that only valid, untampered binaries are executed, preventing attackers from substituting legitimate binaries with malicious ones.
? C. Performing manual updates via USB ports: This is not practical and does not scale well, especially in large environments.
? D. Allowing only files from internal sources: This reduces the risk but does not provide a mechanism to verify the integrity of binaries.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-57, "Recommendation for Key Management"
? OWASP (Open Web Application Security Project) guidelines on code signing

NEW QUESTION 85
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 86
After an incident occurred, a team reported during the lessons-learned review that the team.
* Lost important Information for further analysis.
* Did not utilize the chain of communication
* Did not follow the right steps for a proper response
Which of the following solutions is the best way to address these findinds?

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

Answer: B

Explanation:
Building playbooks for different scenarios and performing regular table-top exercises directly addresses the issues identified in the lessons-learned review. Here's why:
? Lost important information for further analysis: Playbooks outline step-by-step procedures for incident response, ensuring that team members know exactly what to document and how to preserve evidence.
? Did not utilize the chain of communication: Playbooks include communication protocols, specifying who to notify and when. Regular table-top exercises reinforce these communication channels, ensuring they are followed during actual incidents.
? Did not follow the right steps for a proper response: Playbooks provide a clear sequence of actions to be taken during various types of incidents, helping the team to respond in a structured and effective manner. Regular exercises allow the team to practice these steps, identifying and correcting any deviations from the plan.
Investing in better forensic tools (Option A) or requiring certifications (Option C) are also valuable, but they do not directly address the procedural and communication gaps identified. Publishing and enforcing the incident response policy (Option D) is important but not as practical and hands-on as playbooks and exercises in ensuring the team is prepared.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"
? SANS Institute, "Incident Handler's Handbook"

NEW QUESTION 91
A cloud engineer needs to identify appropriate solutions to:
• Provide secure access to internal and external cloud resources.
• Eliminate split-tunnel traffic flows.
• Enable identity and access management capabilities.
Which of the following solutions arc the most appropriate? (Select two).

A. Federation
B. Microsegmentation
C. CASB
D. PAM
E. SD-WAN
F. SASE

Answer: CF

Explanation:
To provide secure access to internal and external cloud resources, eliminate split-tunnel traffic flows, and enable identity and access management capabilities, the most appropriate solutions are CASB (Cloud Access Security Broker) and SASE (Secure Access Service Edge).
Why CASB and SASE?
? CASB (Cloud Access Security Broker):
? SASE (Secure Access Service Edge):
Other options, while useful, do not comprehensively address all the requirements:
? A. Federation: Useful for identity management but does not eliminate split-tunnel traffic or provide comprehensive security.
? B. Microsegmentation: Enhances security within the network but does not directly address secure access to cloud resources or split-tunnel traffic.
? D. PAM (Privileged Access Management): Focuses on managing privileged accounts and does not provide comprehensive access control for internal and external resources.
? E. SD-WAN: Enhances WAN performance but does not inherently provide the identity and access management capabilities or eliminate split-tunnel traffic.
References:
? CompTIA SecurityX Study Guide
? "CASB: Cloud Access Security Broker," Gartner Research

NEW QUESTION 93
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 94
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).

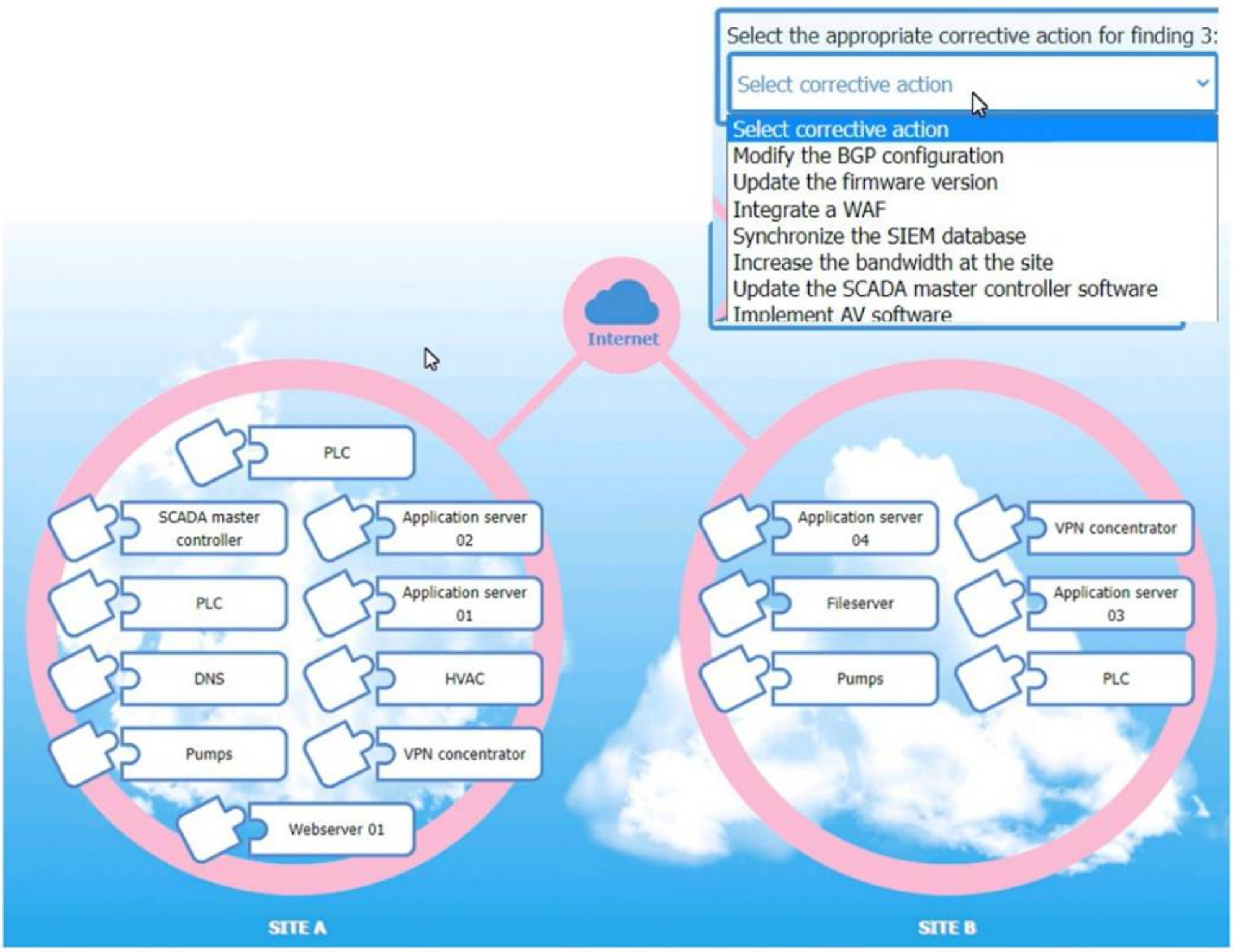
A. Implementing data loss prevention
B. Deploying file integrity monitoring
C. Restricting access to critical file services only
D. Deploying directory-based group policies
E. Enabling modem authentication that supports MFA
F. Implementing a version control system
G. Implementing a CMDB platform

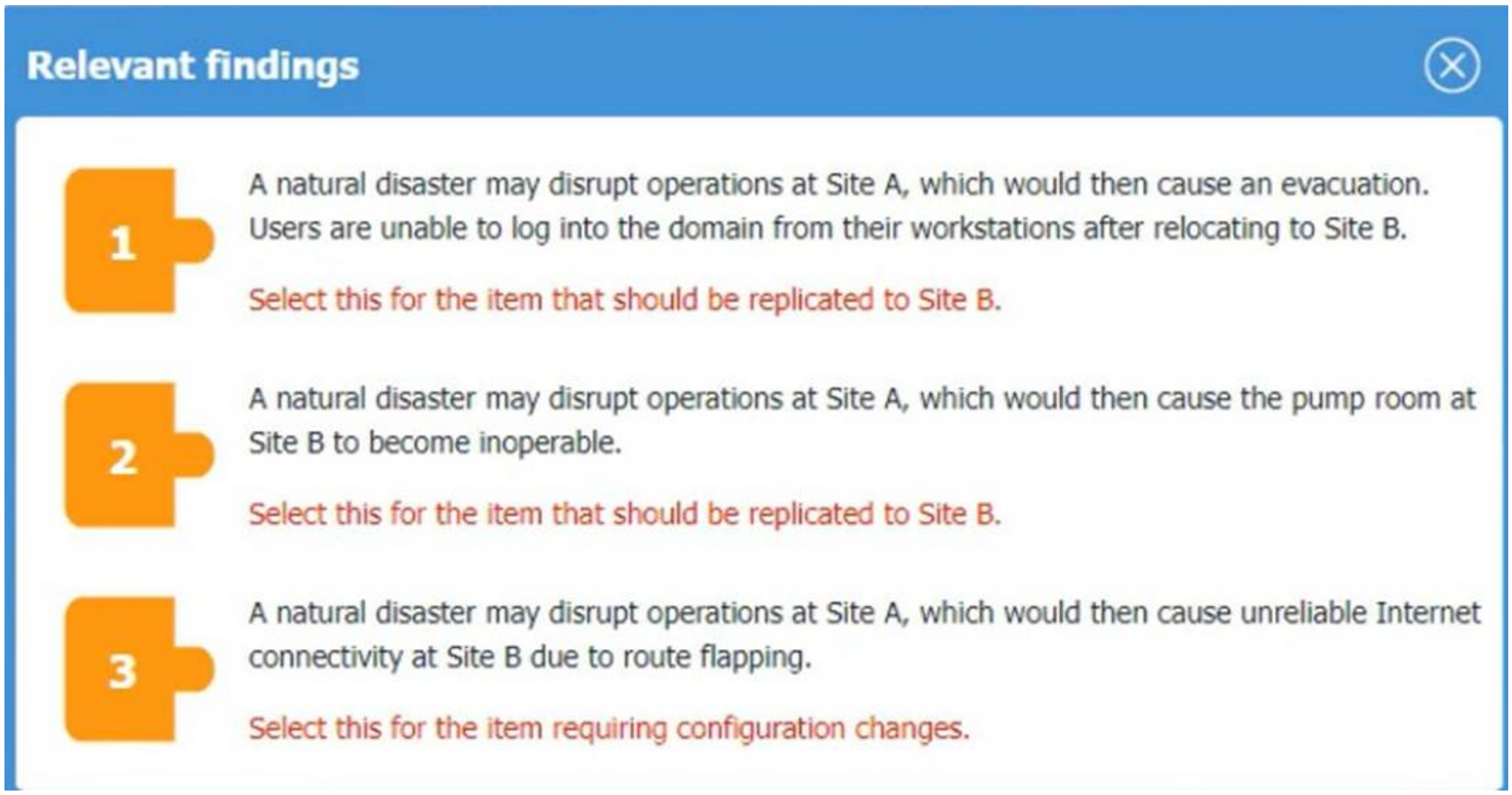
Answer: AE

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 96
SIMULATION
An organization is planning for disaster recovery and continuity of operations, and has noted the following relevant findings:
* 1. A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are
unable to log into the domain from-their workstations after relocating to Site B.
* 2. A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B
to become inoperable.
* 3. A natural disaster may disrupt operations at Site A, which would then cause unreliable internet
connectivity at Site B due to route flapping.
INSTRUCTIONS
Match each relevant finding to the affected host by clicking on the host name and selecting the appropriate number.
For findings 1 and 2, select the items that should be replicated to Site B. For finding 3, select the item requiring configuration changes, then select the appropriate corrective action from the drop-down menu.





A. Mastered
B. Not Mastered

Answer: A

Explanation:
Matching Relevant Findings to the Affected Hosts:
? Finding 1:
? Finding 2:
? Finding 3:
Corrective Actions for Finding 3:
? Finding 3 Corrective Action:
? Replication to Site B for Finding 1:
? Replication to Site B for Finding 2:
? Configuration Changes for Finding 3:
References:
? CompTIA Security+ Study Guide: This guide provides detailed information on disaster recovery and continuity of operations, emphasizing the importance of replicating critical services and making necessary configuration changes to ensure seamless operation during disruptions.
? CompTIA Security+ Exam Objectives: These objectives highlight key areas in disaster recovery planning, including the replication of critical services and network configuration adjustments.
? Disaster Recovery and Business Continuity Planning (DRBCP): This resource outlines best practices for ensuring that operations can continue at an alternate site during a disaster, including the replication of essential services and network stability measures.
By ensuring that critical services like DNS and control systems for pumps are replicated at the alternate site, and by addressing network routing issues through proper BGP configuration, the organization can maintain operational continuity and minimize the impact of natural disasters on their operations.

NEW QUESTION 100
A security architect for a global organization with a distributed workforce recently received funding lo deploy a CASB solution Which of the following most likely explains the choice to use a proxy-based CASB?

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

Answer: A

Explanation:
A proxy-based Cloud Access Security Broker (CASB) is chosen primarily for its ability to block unapproved applications and services. Here??s why:
? Application and Service Control: Proxy-based CASBs can monitor and control the
use of applications and services by inspecting traffic as it passes through the proxy. This allows the organization to enforce policies that block unapproved applications and services, ensuring compliance with security policies.
? Visibility and Monitoring: By routing traffic through the proxy, the CASB can
provide detailed visibility into user activities and data flows, enabling better monitoring and threat detection.
? Real-Time Protection: Proxy-based CASBs can provide real-time protection
against threats by analyzing and controlling traffic before it reaches the end user, thus preventing the use of risky applications and services.
? References:

NEW QUESTION 104

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 106
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 109
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 111
Emails that the marketing department is sending to customers are pomp to the customers' spam folders. The security team is investigating the issue and discovers that the certificates used by the email server were reissued, but DNS records had not been updated. Which of the following should the security team update in order to fix this issue? (Select three.)

A. DMARC
B. SPF
C. DKIM
D. DNSSEC
E. SASC
F. SAN
G. SOA
H. MX

Answer: ABC

Explanation:
To prevent emails from being marked as spam, several DNS records related to email authentication need to be properly configured and updated when there are changes to the email server's certificates:
? A. DMARC (Domain-based Message Authentication, Reporting & Conformance):
DMARC records help email servers determine how to handle messages that fail SPF or DKIM checks, improving email deliverability and reducing the likelihood of emails being marked as spam.
? B. SPF (Sender Policy Framework): SPF records specify which mail servers are authorized to send email on behalf of your domain. Updating the SPF record ensures that the new email server is recognized as an authorized sender.
? C. DKIM (DomainKeys Identified Mail): DKIM adds a digital signature to email
headers, allowing the receiving server to verify that the email has not been tampered with and is from an authorized sender. Updating DKIM records ensures that emails are properly signed and authenticated.
? D. DNSSEC (Domain Name System Security Extensions): DNSSEC adds security
to DNS by enabling DNS responses to be verified. While important for DNS security, it does not directly address the issue of emails being marked as spam.
? E. SASC: This is not a relevant standard for this scenario.
? F. SAN (Subject Alternative Name): SAN is used in SSL/TLS certificates for securing multiple domain names, not for email delivery issues.
? G. SOA (Start of Authority): SOA records are used for DNS zone administration and do not directly impact email deliverability.
? H. MX (Mail Exchange): MX records specify the mail servers responsible for receiving email on behalf of a domain. While important, the primary issue here is the authentication of outgoing emails, which is handled by SPF, DKIM, and DMARC.
References:
? CompTIA Security+ Study Guide
? RFC 7208 (SPF), RFC 6376 (DKIM), and RFC 7489 (DMARC)
? NIST SP 800-45, "Guidelines on Electronic Mail Security"

NEW QUESTION 112
A security analyst is troubleshooting the reason a specific user is having difficulty accessing company resources The analyst reviews the following information:

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

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

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

Answer: B

Explanation:
The table shows that the user "SALES1" is consistently blocked despite having met the MFA requirements. The common factor in these blocked attempts is the source IP address (8.11.4.16) being identified as from Germany while the user is assigned to France. This discrepancy suggests that the network geolocation is being misidentified by the authentication server, causing legitimate access attempts to be blocked.
Why Network Geolocation Misidentification?
? Geolocation Accuracy: Authentication systems often use IP geolocation to verify the location of access attempts. Incorrect geolocation data can lead to legitimate requests being denied if they appear to come from unexpected locations.
? Security Policies: Company security policies might block access attempts from certain locations to prevent unauthorized access. If the geolocation is wrong, legitimate users can be inadvertently blocked.
? Consistent Pattern: The user "SALES1" from the IP address 8.11.4.16 is always blocked, indicating a consistent issue with geolocation.
Other options do not align with the pattern observed:
? A. Bypass MFA requirements: MFA is satisfied, so bypassing MFA is not the issue.
? C. Administrator access policy: This is about user access, not specific administrator access.
? D. OTP codes: The user has satisfied MFA, so OTP code configuration is not the issue.
References:
? CompTIA SecurityX Study Guide
? "Geolocation and Authentication," NIST Special Publication 800-63B

? "IP Geolocation Accuracy," Cisco Documentation

NEW QUESTION 114
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 118
A hospital provides tablets to its medical staff to enable them to more quickly access and edit patients' charts. The hospital wants to ensure that if a tablet is Identified as lost or stolen and a remote command is issued, the risk of data loss can be mitigated within seconds. The tablets are configured as follows to meet hospital policy
• Full disk encryption is enabled
• "Always On" corporate VPN is enabled
• ef-use-backed keystore is enabled'ready.
• Wi-Fi 6 is configured with SAE.
• Location services is disabled.
•Application allow list is configured

A. Revoking the user certificates used for VPN and Wi-Fi access
B. Performing cryptographic obfuscation
C. Using geolocation to find the device
D. Configuring the application allow list to only per mil emergency calls
E. Returning on the device's solid-state media to zero

Answer: E

Explanation:
To mitigate the risk of data loss on a lost or stolen tablet quickly, the most effective strategy is to return the device's solid-state media to zero, which effectively erases all data on the device. Here's why:
? Immediate Data Erasure: Returning the solid-state media to zero ensures that all
data is wiped instantly, mitigating the risk of data loss if the device is lost or stolen.
? Full Disk Encryption: Even though the tablets are already encrypted, physically erasing the data ensures that no residual data can be accessed if someone attempts to bypass encryption.
? Compliance and Security: This method adheres to best practices for data security and compliance, ensuring that sensitive patient data cannot be accessed by unauthorized parties.

NEW QUESTION 119
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 120
A network engineer must ensure that always-on VPN access is enabled Curt restricted to company assets Which of the following best describes what the engineer needs to do"

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

Answer: A

Explanation:
To ensure always-on VPN access is enabled and restricted to company assets, the network engineer needs to generate device certificates using the specific template settings required for the company's VPN solution. These certificates ensure that only authorized devices can establish a VPN connection.
Why Device Certificates are Necessary:
? Authentication: Device certificates authenticate company assets, ensuring that only authorized devices can access the VPN.
? Security: Certificates provide a higher level of security compared to username and password combinations, reducing the risk of unauthorized access.
? Compliance: Certificates help in meeting security policies and compliance requirements by ensuring that only managed devices can connect to the corporate network.
Other options do not provide the same level of control and security for always-on VPN access:
? B. Modify signing certificates for IKE version 2: While important for VPN protocols,
it does not address device-specific authentication.
? C. Create a wildcard certificate: This is not suitable for device-specific authentication and could introduce security risks.
? D. Add the VPN hostname as a SAN entry: This is more related to certificate management and does not ensure device-specific authentication.
References:
? CompTIA SecurityX Study Guide
? "Device Certificates for VPN Access," Cisco Documentation
? NIST Special Publication 800-77, "Guide to IPsec VPNs"

NEW QUESTION 124
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 129
A security engineer needs 10 secure the OT environment based on me following requirements
• Isolate the OT network segment
• Restrict Internet access.

• Apply security updates two workstations
• Provide remote access to third-party vendors
Which of the following design strategies should the engineer implement to best meet these requirements?

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

Answer: B

Explanation:
To secure the Operational Technology (OT) environment based on the given requirements, the best approach is to implement a bastion host in the OT network. The bastion host serves as a secure entry point for remote access, allowing third-party vendors to connect
while being monitored by security tools. Using a dedicated update server for workstations ensures that security updates are applied in a controlled manner without direct internet access.
References:
? CompTIA SecurityX Study Guide: Recommends the use of bastion hosts and dedicated update servers for securing OT environments.
? NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security": Advises on isolating OT networks and using secure remote access methods.
? "Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill: Discusses strategies for securing OT networks, including the use of bastion hosts and update servers.

NEW QUESTION 130
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 131
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 136
A company updates its cloud-based services by saving infrastructure code in a remote repository. The code is automatically deployed into the development environment every time the code is saved lo the repository The developers express concern that the deployment often fails, citing minor code issues and occasional security control check failures in the development environment Which of the following should a security engineer recommend to reduce the deployment failures? (Select two).

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

Answer: BD

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

NEW QUESTION 140
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?

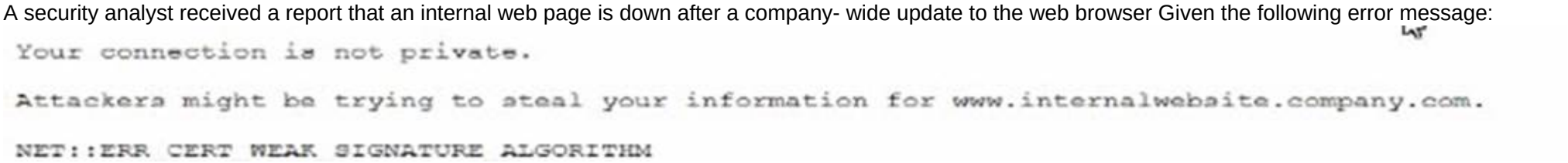
A. Automate alerting to IT support for phone system outages.
B. Enable dashboards for service status monitoring
C. Send emails for failed log-In attempts on the public website
D. Configure automated Isolation of human resources systems

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 143
A security analyst received a report that an internal web page is down after a company- wide update to the web browser Given the following error message:



Which of the following is the b«« way to fix this issue?

A. Rewriting any legacy web functions
B. Disabling all deprecated ciphers
C. Blocking all non-essential pons
D. Discontinuing the use of self-signed certificates

Answer: D

Explanation:
The error message "NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM" indicates that the web browser is rejecting the certificate because it uses a weak signature algorithm. This commonly happens with self-signed certificates, which often use outdated or insecure algorithms.
Why Discontinue Self-Signed Certificates?
? Security Compliance: Modern browsers enforce strict security standards and may reject certificates that do not comply with these standards.
? Trusted Certificates: Using certificates from a trusted Certificate Authority (CA) ensures compliance with security standards and is less likely to be flagged as insecure.
? Weak Signature Algorithm: Self-signed certificates might use weak algorithms like MD5 or SHA-1, which are considered insecure.
Other options do not address the specific cause of the certificate error:
? A. Rewriting legacy web functions: Does not address the certificate issue.
? B. Disabling deprecated ciphers: Useful for improving security but not related to the certificate error.
? C. Blocking non-essential ports: This is unrelated to the issue of certificate validation.
References:
? CompTIA SecurityX Study Guide
? "Managing SSL/TLS Certificates," OWASP
? "Best Practices for Certificate Management," NIST Special Publication 800-57

NEW QUESTION 147
.....

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