CompTIA

Exam Questions CAS-005

CompTIA SecurityX Exam

NEW QUESTION 1
A company wants to implement hardware security key authentication for accessing sensitive information systems The goal is to prevent unauthorized users from gaining access with a stolen password Which of the following models should the company implement to b«st solve this issue?

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

Answer: D

Explanation:
Context-based authentication enhances traditional security methods by incorporating additional layers of information about the user's current environment and behavior. This can include factors such as the user's location, the time of access, the device used, and the behavior patterns. It is particularly useful in preventing unauthorized access even if an attacker has obtained a valid password.
? Rule-based (A) focuses on predefined rules and is less flexible in adapting to dynamic threats.
? Time-based (B) authentication considers the time factor but doesn't provide comprehensive protection against stolen credentials.
? Role-based (C) is more about access control based on the user's role within the organization rather than authenticating the user based on current context.
By implementing context-based authentication, the company can ensure that even if a password is compromised, the additional contextual factors required for access (which an attacker is unlikely to possess) provide a robust defense mechanism.
References:
? CompTIA SecurityX guide on authentication models and best practices.
? NIST guidelines on authentication and identity proofing.
? Analysis of multi-factor and adaptive authentication techniques.

NEW QUESTION 2
A company's help desk is experiencing a large number of calls from the finance department slating access issues to www bank com The security operations center reviewed the following security logs:

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

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

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

Answer: C

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

NEW QUESTION 3
Which of the following best explains the business requirement a healthcare provider fulfills by encrypting patient data at rest?

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

Answer: D

Explanation:
Encrypting patient data at rest is a critical requirement for healthcare providers to ensure compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The primary business requirement fulfilled by this practice is the protection of patient privacy while supporting the portability of medical

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

NEW QUESTION 4
An organization wants to implement a platform to better identify which specific assets are affected by a given vulnerability. Which of the following components provides the best foundation to achieve this goal?

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

Answer: B

Explanation:
A Configuration Management Database (CMDB) provides the best foundation for identifying which specific assets are affected by a given vulnerability. A CMDB maintains detailed information about the IT environment, including hardware, software, configurations, and relationships between assets. This comprehensive view allows organizations to quickly identify and address vulnerabilities affecting specific assets. References:
? CompTIA SecurityX Study Guide: Discusses the role of CMDBs in asset management and vulnerability identification.
? ITIL (Information Technology Infrastructure Library) Framework: Recommends the
use of CMDBs for effective configuration and asset management.
? "Configuration Management Best Practices" by Bob Aiello and Leslie Sachs: Covers the importance of CMDBs in managing IT assets and addressing vulnerabilities.

NEW QUESTION 5
A company is having issues with its vulnerability management program New devices/lPs 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 6
A company detects suspicious activity associated with external connections Security detection tools are unable to categorize this activity. Which of the following is the best solution to help the company overcome this challenge?

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

Answer: D

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

NEW QUESTION 7
A news organization wants to implement workflows that allow users to request that untruthful data be retraced and scrubbed from online publications to comply with the right to be forgotten Which of the following regulations is the organization most likely trying to address'

A. GDPR
B. COPPA
C. CCPA

D. DORA

Answer: A

Explanation:
The General Data Protection Regulation (GDPR) is the regulation most likely being addressed by the news organization. GDPR includes provisions for the "right to be forgotten," which allows individuals to request the deletion of personal data that is no longer necessary for the purposes for which it was collected. This regulation aims to protect the privacy and personal data of individuals within the European Union.
References:
? CompTIA SecurityX Study Guide: Covers GDPR and its requirements, including the right to be forgotten.
? GDPR official documentation: Details the rights of individuals, including data erasure and the right to be forgotten.
? "GDPR: A Practical Guide to the General Data Protection Regulation" by IT Governance Privacy Team: Provides a comprehensive overview of GDPR compliance, including workflows for data deletion requests.

NEW QUESTION 8
A company's SICM Is continuously reporting false positives and false negatives The security operations team has Implemented configuration changes to troubleshoot possible reporting errors Which of the following sources of information best supports the required analysts process? (Select two).

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

Answer: AB

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

NEW QUESTION 9
A company wants to use loT devices to manage and monitor thermostats at all facilities The thermostats must receive vendor security updates and limit access to other devices within the organization Which of the following best addresses the company's requirements"

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

Answer: B

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

NEW QUESTION 10
SIMULATION
You are a security analyst tasked with interpreting an Nmap scan output from company??s privileged network.
The company??s hardening guidelines indicate the following: There should be one primary server or service per device. Only default ports should be used. Non-secure protocols should be disabled.
INSTRUCTIONS
Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.
For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:
The IP address of the device
The primary server or service of the device (Note that each IP should by associated with one service/port only)
The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines)
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

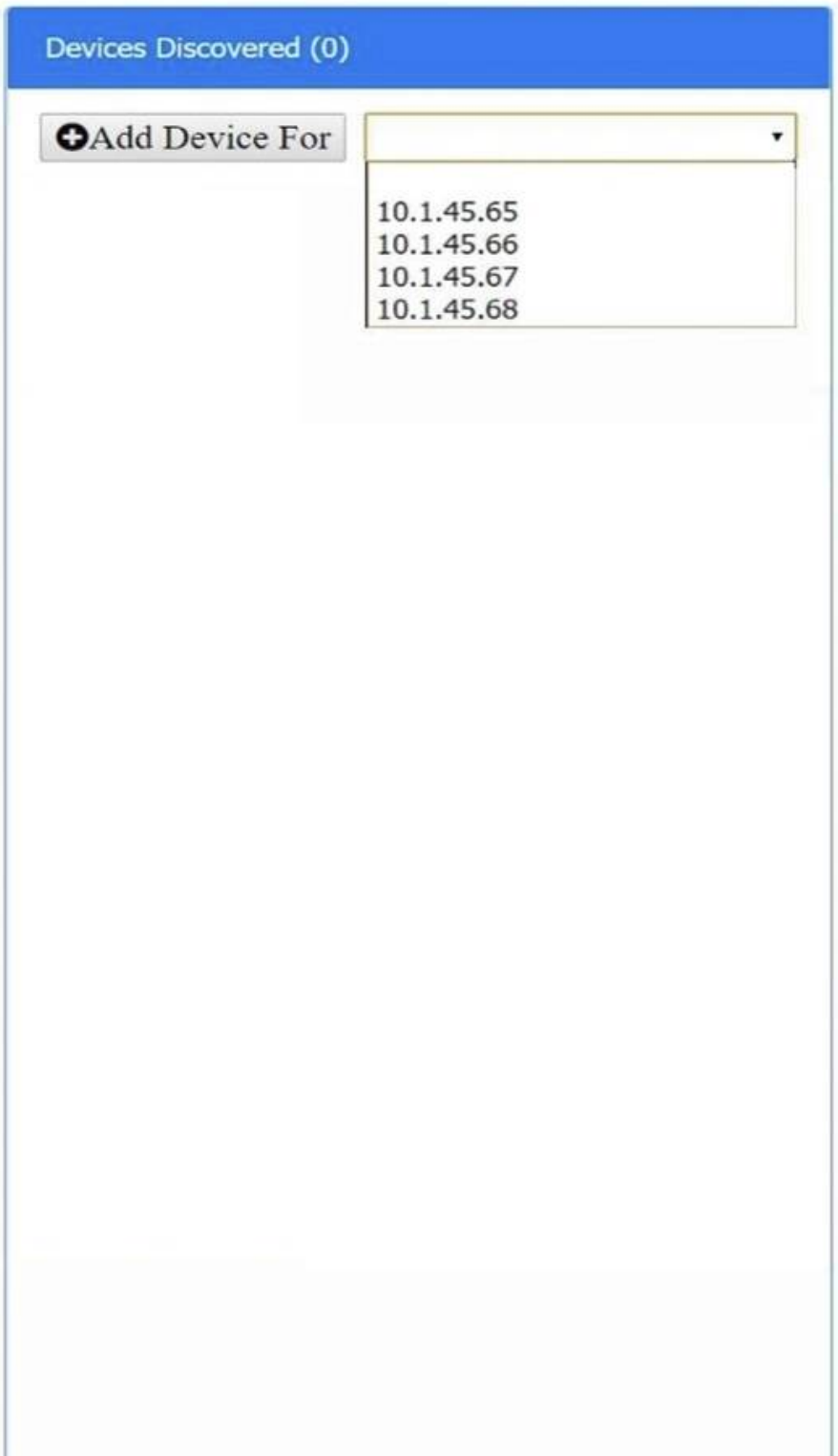
NMAP Scan Output

```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT     STATE  SERVICE  VERSION
25/tcp   closed smtp     Barracuda Networks Spam Firewall smtpd
415/tcp  open   ssl/smtp smtpd
587/tcp  open   ssl/smtp smtpd
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE  VERSION
20/tcp   closed ftp-data
21/tcp   open   ftp      FileZilla ftpd 0.9.39 beta
22/tcp   closed ssh
80/tcp   open   http     Microsoft IIS httpd 7.5
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            Pure-FTPd
443/tcp  open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
```



A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 10.1.45.65 SFTP Server Disable 8080
* 10.1.45.66 Email Server Disable 415 and 443
* 10.1.45.67 Web Server Disable 21, 80
* 10.1.45.68 UTM Appliance Disable 21

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

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

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

A. OW1N23 uses a legacy version of Windows that is not supported by the EDR
B. LN002 was not supported by the EDR solution and propagates the RAT
C. The EDR has an unknown vulnerability that was exploited by the attacker.
D. 0W1N29 spreads the malware through other hosts in the network

Answer: A

Explanation:
OWIN23 is running Windows 7, which is a legacy operating system. Many EDR solutions no longer provide full support for outdated operating systems like Windows 7, which has reached its end of life and is no longer receiving security updates from Microsoft. This makes such systems more vulnerable to infections and attacks, including remote access Trojans (RATs).
? A. OWIN23 uses a legacy version of Windows that is not supported by the EDR:
This is the most probable cause because the lack of support means that the EDR solution may not fully protect or monitor this system, making it an easy target for infections.
? B. LN002 was not supported by the EDR solution and propagates the RAT: While LN002 is unmanaged, it is less likely to propagate the RAT to OWIN23 directly without an established vector.
? C. The EDR has an unknown vulnerability that was exploited by the attacker: This is possible but less likely than the lack of support for an outdated OS.
? D. OWIN29 spreads the malware through other hosts in the network: While this could happen, the status indicates OWIN29 is in a bypass mode, which might limit its interactions but does not directly explain the infection on OWIN23.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations"
? Microsoft's Windows 7 End of Support documentation

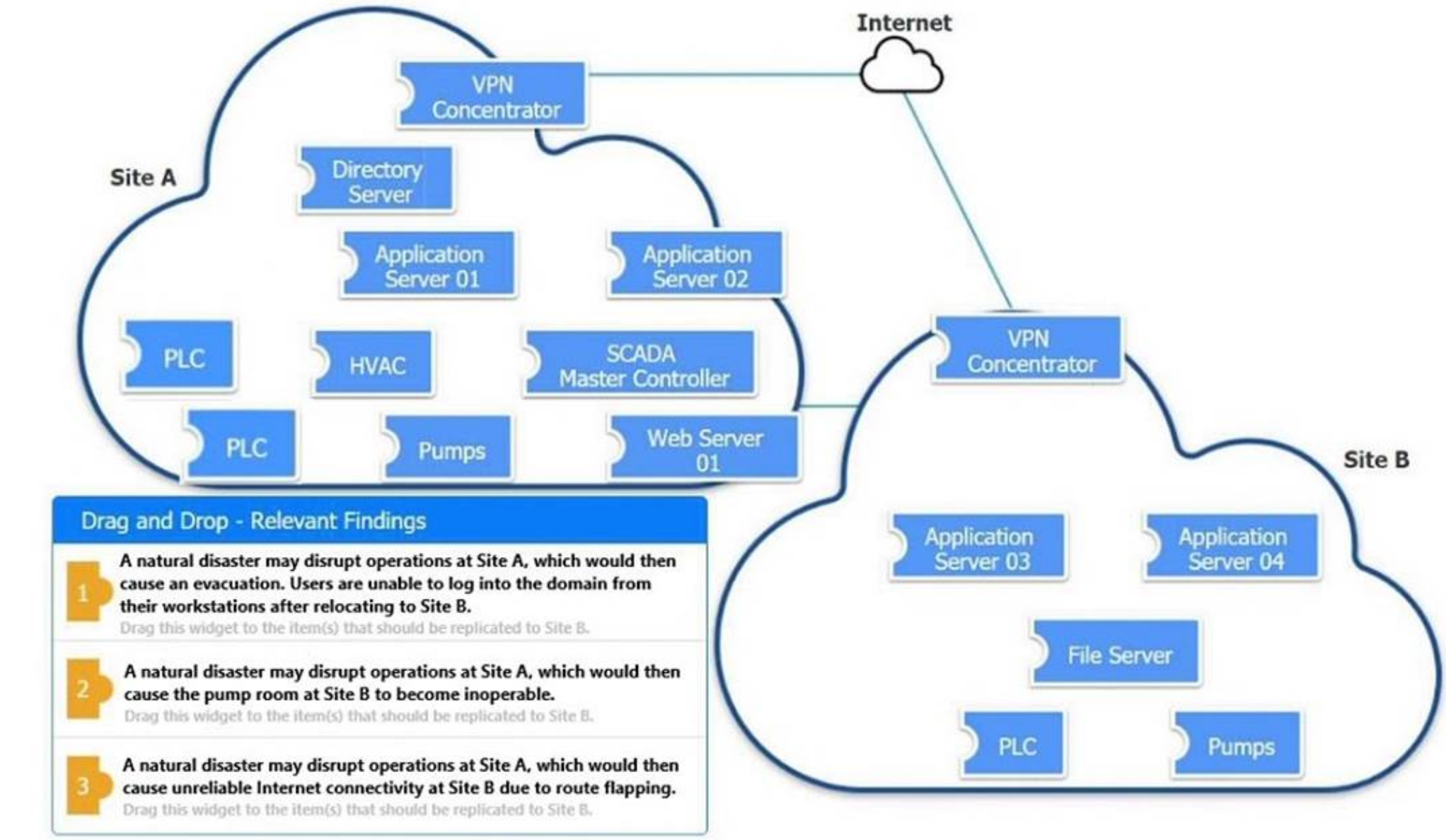
NEW QUESTION 11
A security officer received several complaints from users about excessive MPA push notifications at night The security team investigates and suspects malicious activities regarding user account authentication Which of the following is the best way for the security officer to restrict 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

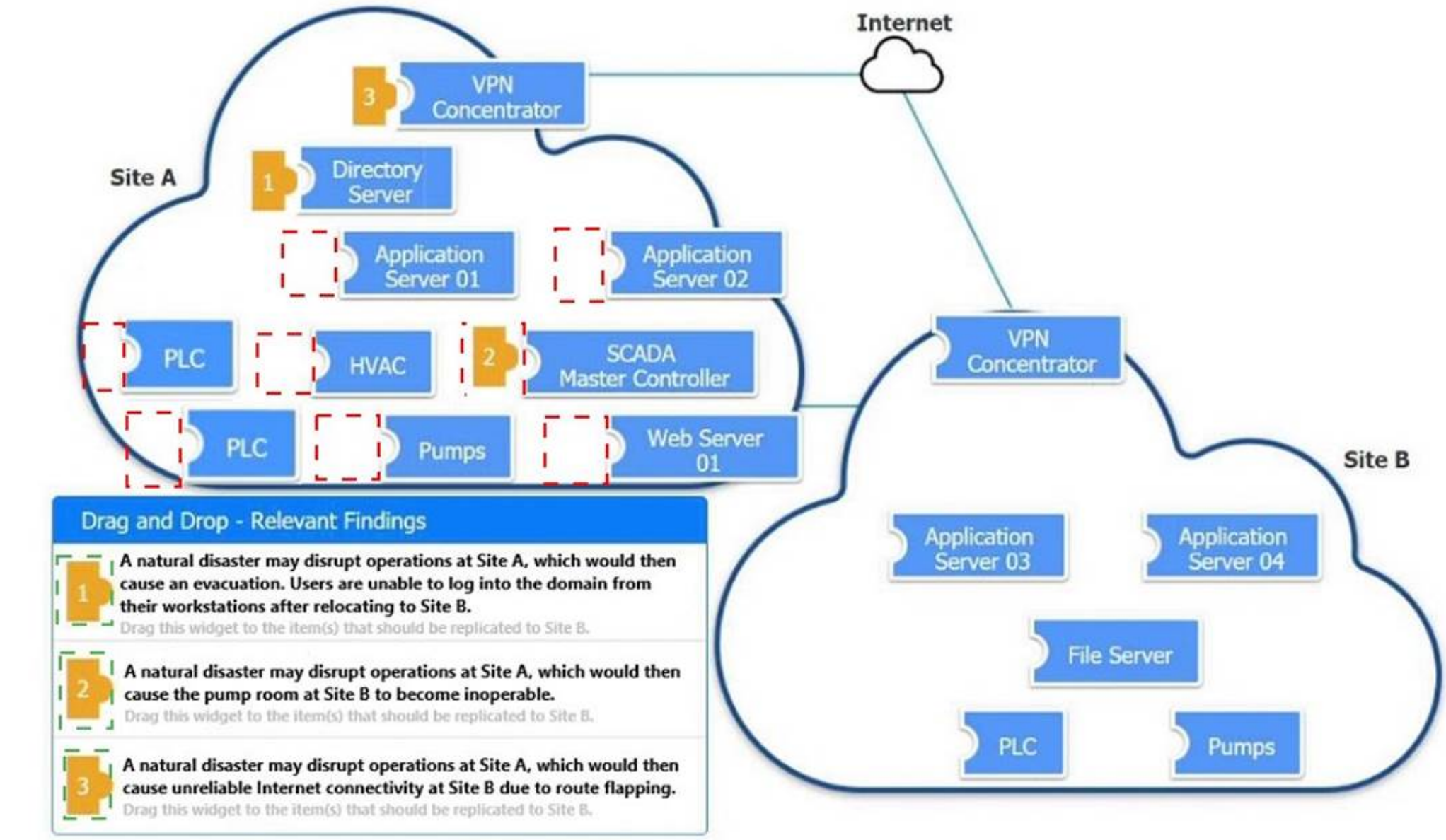
Answer: D

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 13
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 14
Developers have been creating and managing cryptographic material on their personal laptops fix use in production environment. A security engineer needs to initiate a more secure process. Which of the following is the best strategy for the engineer to use?

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

Answer: D

Explanation:
The best strategy for securely managing cryptographic material is to use a Hardware Security Module (HSM). Here??s why:
? Security and Integrity: HSMs are specialized hardware devices designed to protect and manage digital keys. They provide high levels of physical and logical security, ensuring that cryptographic material is well protected against tampering and unauthorized access.
? Centralized Key Management: Using HSMs allows for centralized management of cryptographic keys, reducing the risks associated with decentralized and potentially insecure key storage practices, such as on personal laptops.
? Compliance and Best Practices: HSMs comply with various industry standards and regulations (such as FIPS 140-2) for secure key management. This ensures that the organization adheres to best practices and meets compliance requirements.
? References:

NEW QUESTION 17
A security analyst received a notification from a cloud service provider regarding an attack detected on a web server The cloud service provider shared the following information about the attack:
• The attack came from inside the network.
• The attacking source IP was from the internal vulnerability scanners.
• The scanner is not configured to target the cloud servers.
Which of the following actions should the security analyst take first?

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

Answer: D

Explanation:
When a security analyst receives a notification about an attack that appears to originate from an internal vulnerability scanner, it suggests that the scanner itself might have been compromised. This situation is critical because a compromised scanner can potentially conduct unauthorized scans, leak sensitive information, or execute malicious actions within the network. The appropriate first action involves containing the threat to prevent further damage and allow for a thorough investigation.
Here??s why quarantining the scanner sensor is the best immediate action:
? Containment and Isolation: Quarantining the scanner will immediately prevent it
from continuing any malicious activity or scans. This containment is crucial to protect the rest of the network from potential harm.
? Forensic Analysis: By isolating the scanner, a forensic analysis can be performed to understand how it was compromised, what actions it took, and what data or systems might have been affected. This analysis will provide valuable insights into the nature of the attack and help in taking appropriate remedial actions.
? Preventing Further Attacks: If the scanner is allowed to continue operating, it might execute more unauthorized actions, leading to greater damage. Quarantine ensures that the threat is neutralized promptly.
? Root Cause Identification: A forensic analysis can help identify vulnerabilities in the scanner??s configuration, software, or underlying system that allowed the compromise. This information is essential for preventing future incidents.
Other options, while potentially useful in the long term, are not appropriate as immediate actions in this scenario:
? A. Create an allow list for the vulnerability scanner IPs to avoid false positives:
This action addresses false positives but does not mitigate the immediate threat posed by the compromised scanner.
? B. Configure the scan policy to avoid targeting an out-of-scope host: This step is preventive for future scans but does not deal with the current incident where the scanner is already compromised.
? C. Set network behavior analysis rules: While useful for ongoing monitoring and detection, this does not address the immediate need to stop the compromised scanner??s activities.
In conclusion, the first and most crucial action is to quarantine the scanner sensor to halt any malicious activity and perform a forensic analysis to understand the

scope and nature of the compromise. This step ensures that the threat is contained and provides a basis for further remediation efforts.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"

NEW QUESTION 19
A security engineer is developing a solution to meet the following requirements?
• All endpoints should be able to establish telemetry with a SIEM.
• All endpoints should be able to be integrated into the XDR platform.
• SOC services should be able to monitor the XDR platform
Which of the following should the security engineer implement to meet the requirements?

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

Answer: D

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

NEW QUESTION 20
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 22
An audit finding reveals that a legacy platform has not retained loos for more than 30 days The platform has been segmented due to its interoperability with newer technology. As a temporary solution, the IT department changed the log retention to 120 days. Which of the following should the security engineer do to ensure the logs are being properly retained?

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

Answer: C

Explanation:
To ensure that logs from a legacy platform are properly retained beyond the default retention period, configuring the SIEM to aggregate the logs is the best approach. SIEM solutions are designed to collect, aggregate, and store logs from various sources, providing centralized log management and retention. This setup ensures that logs are retained according to policy and can be easily accessed for analysis and compliance purposes. References:
? CompTIA SecurityX Study Guide: Discusses the role of SIEM in log management and retention.
? NIST Special Publication 800-92, "Guide to Computer Security Log Management": Recommends the use of centralized log management solutions, such as SIEM, for effective log retention and analysis.
? "Security Information and Event Management (SIEM) Implementation" by David Miller: Covers best practices for configuring SIEM systems to aggregate and retain logs from various sources.

NEW QUESTION 24
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 26
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 27
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 28
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 30
A compliance officer is reviewing the data sovereignty laws in several countries where the organization has no presence Which of the following is the most likely reason for reviewing these laws?

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

Answer: C

Explanation:
Reviewing data sovereignty laws in countries where the organization has no presence is likely due to concerns about regulatory enforcement. Data sovereignty laws dictate how data can be stored, processed, and transferred across borders. Understanding these laws is crucial for compliance, especially if the organization handles data that may be subject to foreign regulations.
? A. The organization is performing due diligence of potential tax issues: This is less likely as tax issues are generally not directly related to data sovereignty laws.
? B. The organization has been subject to legal proceedings in countries where it has a presence: While possible, this does not explain the focus on countries where the organization has no presence.
? C. The organization is concerned with new regulatory enforcement in other countries: This is the most likely reason. New regulations could impact the organization??s operations, especially if they involve data transfers or processing data from these countries.
? D. The organization has suffered brand reputation damage from incorrect media coverage: This is less relevant to the need for reviewing data sovereignty laws.
References:
? CompTIA Security+ Study Guide
? GDPR and other global data protection regulations
? "Data Sovereignty: The Future of Data Protection?" by Mark Burdon

NEW QUESTION 32
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 34
An organization wants to create a threat model to identity vulnerabilities in its infrastructure. Which of the following, should be prioritized first?

A. External-facing Infrastructure with known exploited vulnerabilities
B. Internal infrastructure with high-seventy and Known exploited vulnerabilities
C. External facing Infrastructure with a low risk score and no known exploited vulnerabilities
D. External-facing infrastructure with a high risk score that can only be exploited with local access to the resource

Answer: A

Explanation:
When creating a threat model to identify vulnerabilities in an organization's infrastructure, prioritizing external-facing infrastructure with known exploited vulnerabilities is critical. Here??s why:
? Exposure to Attack: External-facing infrastructure is directly exposed to the
internet, making it a primary target for attackers. Any vulnerabilities in this layer pose an immediate risk to the organization's security.
? Known Exploited Vulnerabilities: Vulnerabilities that are already known and
exploited in the wild are of higher concern because they are actively being used by attackers. Addressing these vulnerabilities reduces the risk of exploitation significantly.
? Risk Mitigation: By prioritizing external-facing infrastructure with known exploited
vulnerabilities, the organization can mitigate the most immediate and impactful threats, thereby improving overall security posture.
? References:

NEW QUESTION 36
A security analyst reviews the following report:

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

Which of the following assessments is the analyst performing?

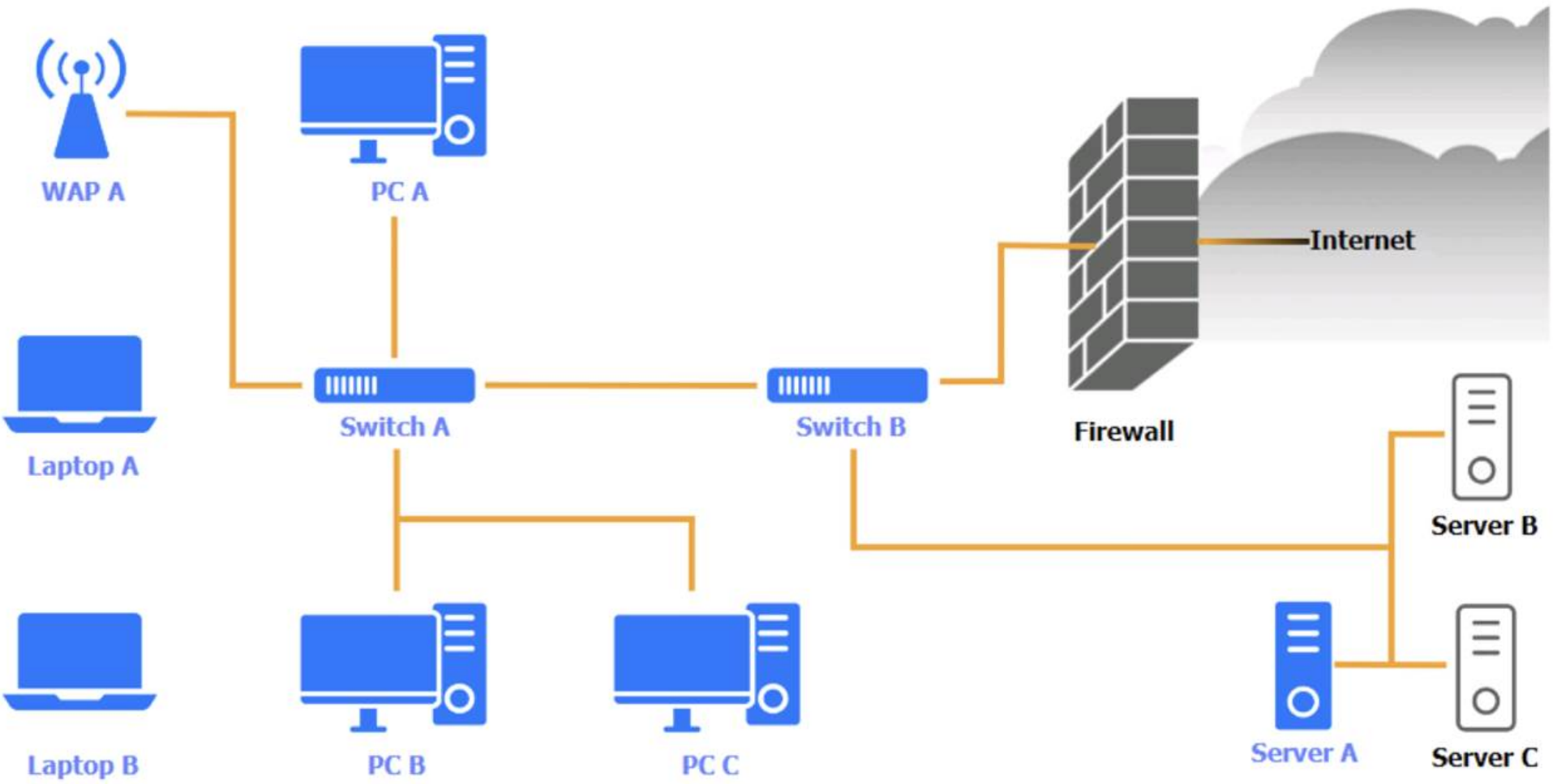
A. System
B. Supply chain
C. Quantitative
D. Organizational

Answer: B

Explanation:
The table shows detailed information about products, including location, chassis manufacturer, OS, application developer, and vendor. This type of information is typically assessed in a supply chain assessment to evaluate the security and reliability of components and services from different suppliers.
Why Supply Chain Assessment?
? Component Evaluation: Assessing the origin and security of each component used in the products, including hardware, software, and third-party services.
? Vendor Reliability: Evaluating the security practices and reliability of vendors involved in providing components or services.
? Risk Management: Identifying potential risks associated with the supply chain, such as vulnerabilities in third-party components or insecure development practices.
Other types of assessments do not align with the detailed supplier and component information provided:
? A. System: Focuses on individual system security, not the broader supply chain.
? C. Quantitative: Focuses on numerical risk assessments, not supplier information.
? D. Organizational: Focuses on internal organizational practices, not external
suppliers.
References:
? CompTIA SecurityX Study Guide

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

NEW QUESTION 37
SIMULATION
A security engineer needs to review the configurations of several devices on the network to meet the following requirements:
• The PostgreSQL server must only allow connectivity in the 10.1.2.0/24 subnet.
• The SSH daemon on the database server must be configured to listen to port 4022.
• The SSH daemon must only accept connections from a Single workstation.
• All host-based firewalls must be disabled on all workstations.
• All devices must have the latest updates from within the past eight days.
• All HDDs must be configured to secure data at rest.
• Cleartext services are not allowed.
• All devices must be hardened when possible.
Instructions:
Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found.
Click on Server A to review output data. Select commands in the appropriate tab to remediate connectivity problems to the pOSTGREsql DATABASE VIA ssh



WAP A

WAP A

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

PC A

PC A

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

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

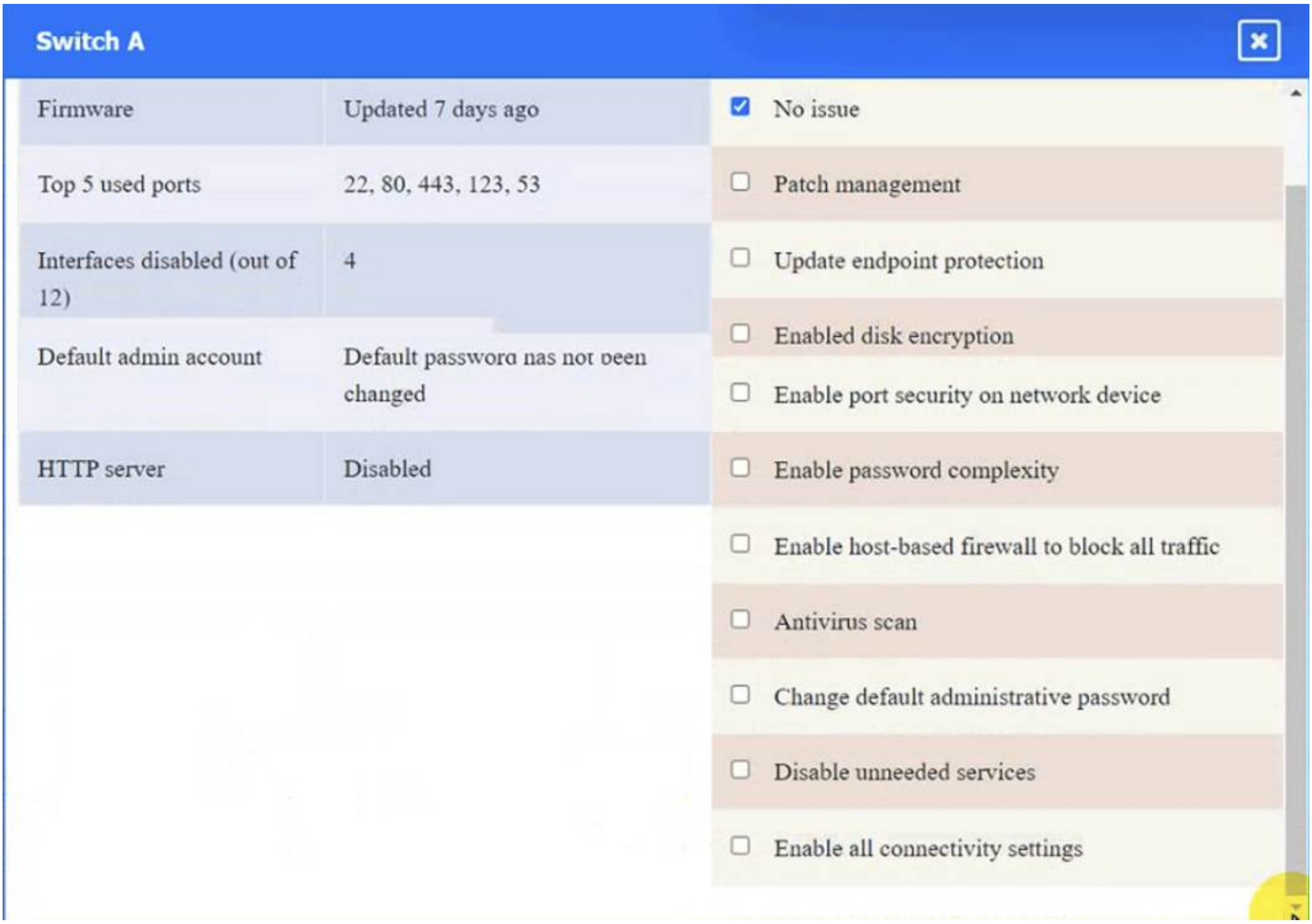
Laptop A

Laptop A

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

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

Switch A



Switch B:

Switch B

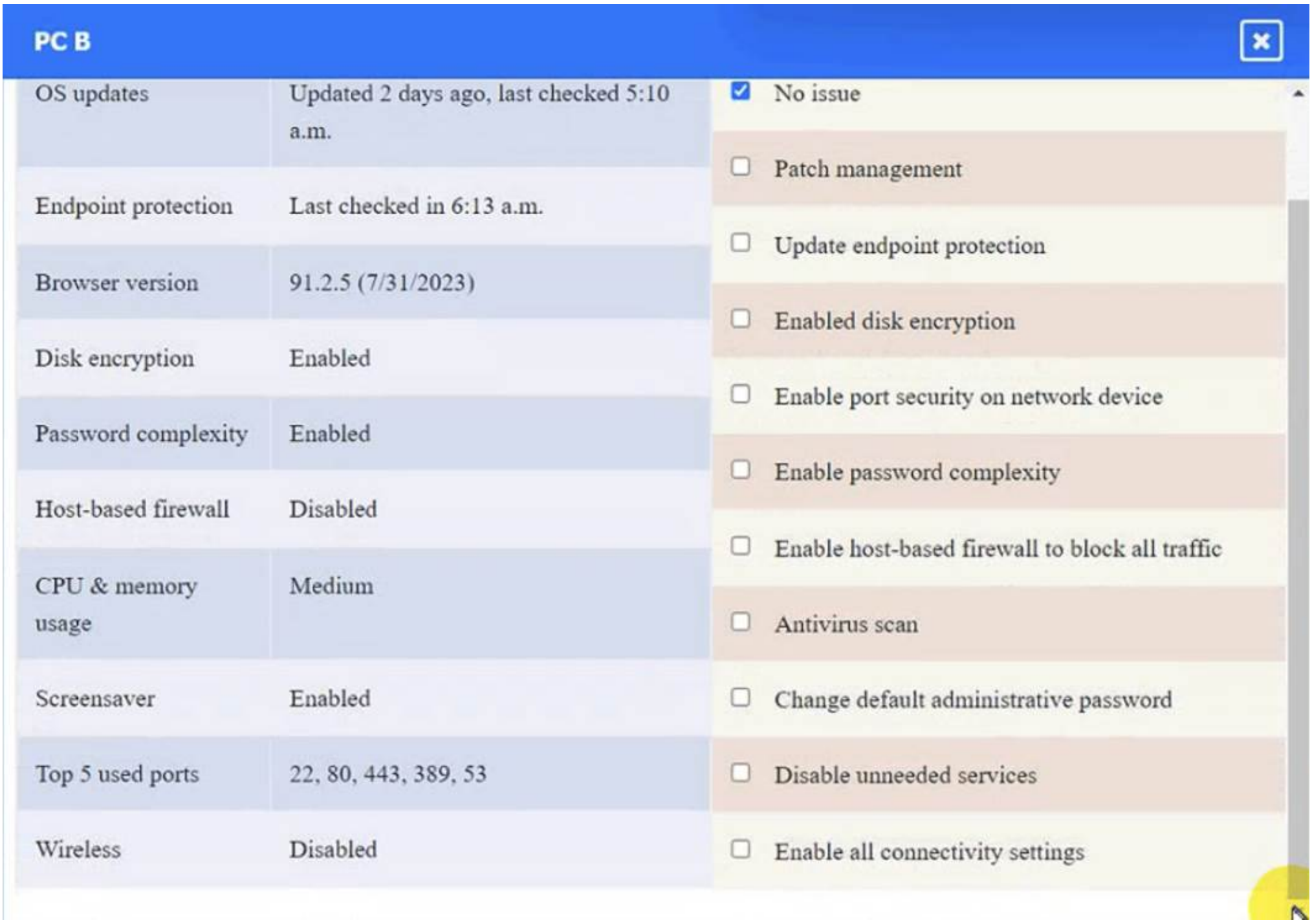
Firmware	Updated 7 days ago	☑ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
Interfaces disabled (out of 6)	1	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
		☐ Enable port security on network device
HTTP server	Disabled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

Laptop B

Laptop B

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

PC B


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

PC C


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

Server A

Server A

Nmap | IP Tables

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

1 2 3 4

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

1 2 3 4

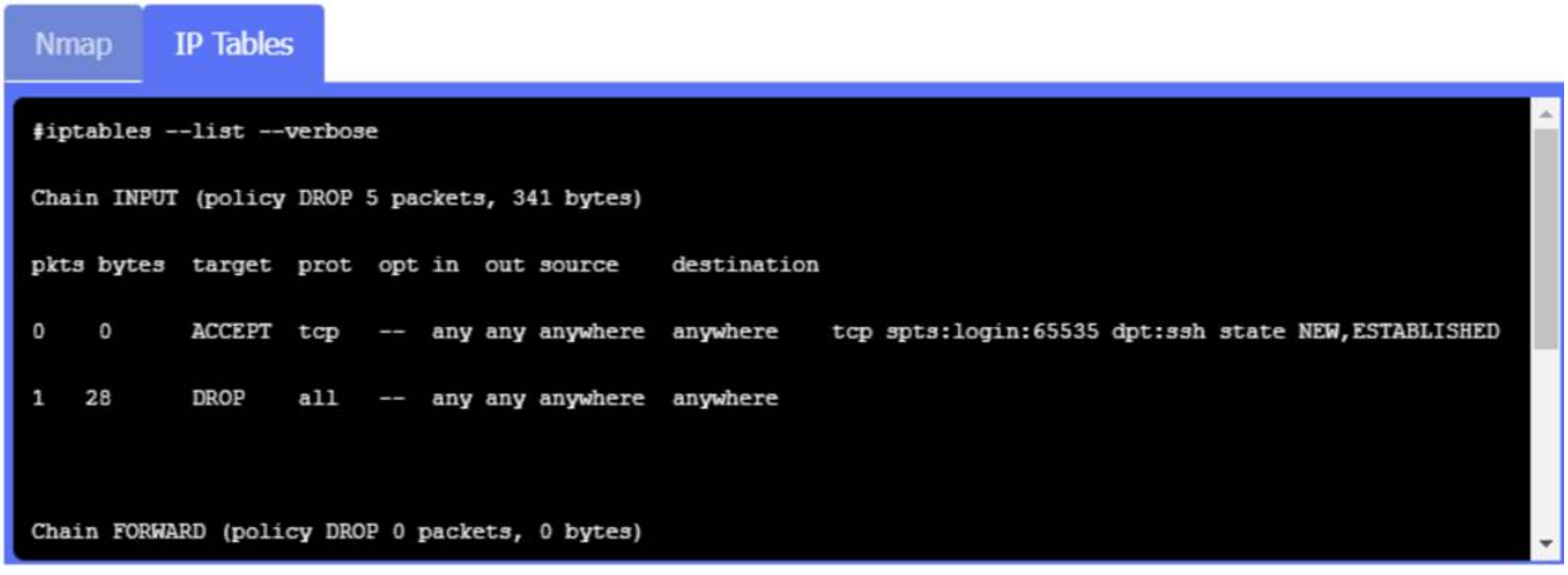
```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

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

1 2 3 4

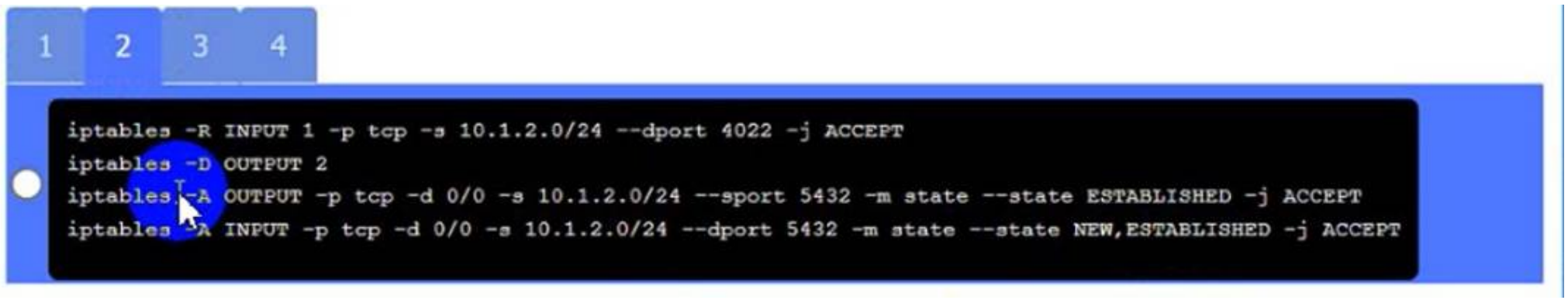
```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --dport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```



A. Mastered
B. Not Mastered

Answer: A

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



NEW QUESTION 40
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 43
A systems administrator wants to introduce a newly released feature for an internal application. The administrate docs not want to test the feature in the production environment. Which of the following locations is the best place to test the new feature?

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

Answer: A

Explanation:
The best location to test a newly released feature for an internal application, without affecting the production environment, is the staging environment. Here??s a detailed Explanation
? Staging Environment: This environment closely mirrors the production environment
in terms of hardware, software, configurations, and settings. It serves as a final testing ground before deploying changes to production. Testing in the staging environment ensures that the new feature will behave as expected in the actual production setup.
? Isolation from Production: The staging environment is isolated from production,
which means any issues arising from the new feature will not impact the live users or the integrity of the production data. This aligns with best practices in change management and risk mitigation.
? Realistic Testing: Since the staging environment replicates the production
environment, it provides realistic testing conditions. This helps in identifying potential issues that might not be apparent in a development or testing environment, which often have different configurations and workloads.
? References:

NEW QUESTION 45
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 48
Third parties notified a company's security team about vulnerabilities in the company's application. The security team determined these vulnerabilities were previously disclosed in third-party libraries. Which of the following solutions best addresses the reported vulnerabilities?

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

Answer: D

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

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

NEW QUESTION 52
A company recently experienced an incident in which an advanced threat actor was able to shim malicious code against the hardware static of a domain controller The forensic team cryptographically validated that com the underlying firmware of the box and the operating system had not been compromised. However, the attacker was able to exfiltrate information from the server using a steganographic technique within LOAP Which of the following is me b»« way to reduce the risk oi reoccurrence?

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

Answer: A

Explanation:
The scenario describes a sophisticated attack where the threat actor used steganography within LDAP to exfiltrate data. Given that the hardware and OS firmware were validated and found uncompromised, the attack vector likely exploited a network communication channel. To mitigate such risks, enforcing allow lists for authorized network ports and protocols is the most effective strategy.
Here??s why this option is optimal:
? Port and Protocol Restrictions: By creating an allow list, the organization can restrict communications to only those ports and protocols that are necessary for legitimate business operations. This reduces the attack surface by preventing unauthorized or unusual traffic.
? Network Segmentation: Enforcing such rules helps in segmenting the network and ensuring that only approved communications occur, which is critical in preventing data exfiltration methods like steganography.
? Preventing Unauthorized Access: Allow lists ensure that only predefined, trusted connections are allowed, blocking potential paths that attackers could use to infiltrate or exfiltrate data.
Other options, while beneficial in different contexts, are not directly addressing the network communication threat:
? B. Measuring and attesting to the entire boot chain: While this improves system
integrity, it doesn??t directly mitigate the risk of data exfiltration through network channels.
? C. Rolling the cryptographic keys used for hardware security modules: This is
useful for securing data and communications but doesn??t directly address the specific method of exfiltration described.
? D. Using code signing to verify the source of OS updates: Ensures updates are
from legitimate sources, but it doesn??t mitigate the risk of network-based data exfiltration.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy"
? CIS Controls Version 8, Control 9: Limitation and Control of Network Ports, Protocols, and Services

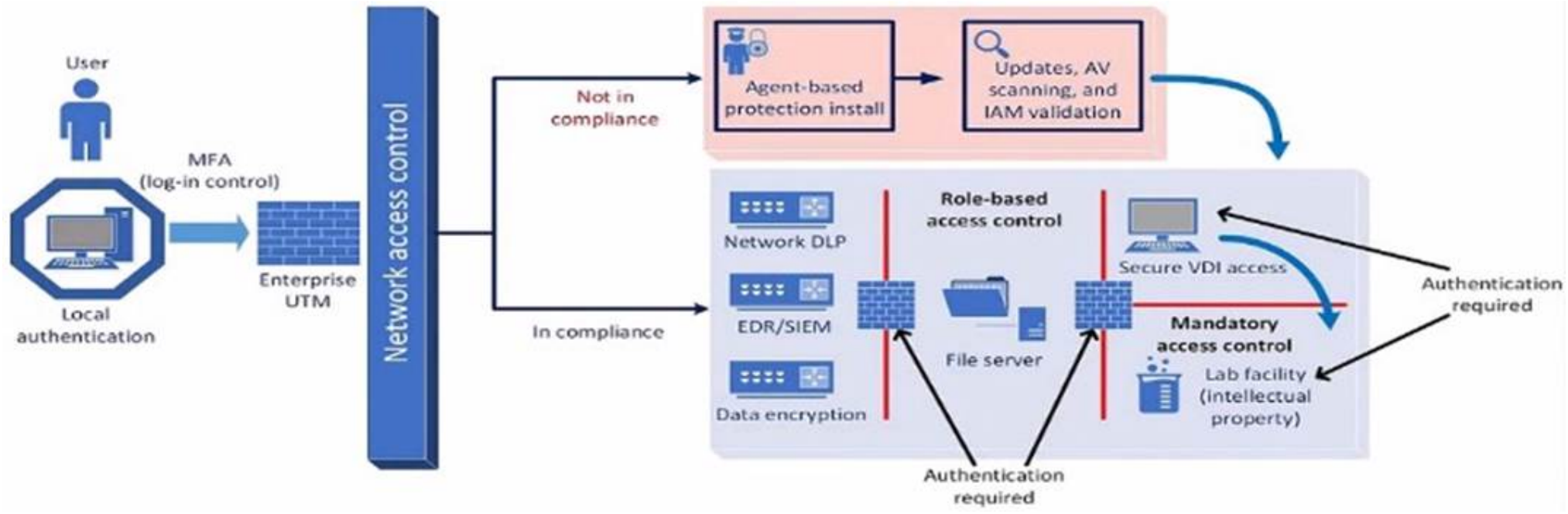
NEW QUESTION 55
A central bank implements strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin. Which of the following best describes the cyberthreat to the bank?

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

Answer: C

Explanation:
The best description of the cyber threat to a central bank implementing strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin, is the risk of physical implants and tampering. Here??s why:
? Supply Chain Security: The supply chain is a critical vector for hardware tampering and physical implants, which can compromise the integrity and security of hardware components before they reach the organization.
? Targeted Attacks: Banks and financial institutions are high-value targets, making
them susceptible to sophisticated attacks, including those involving physical implants that can be introduced during manufacturing or shipping processes.
? Strict Mitigations: Implementing an allow list for specific countries aims to mitigate
the risk of supply chain attacks by limiting the sources of hardware. However, the primary concern remains the introduction of malicious components through tampering.
? References:

NEW QUESTION 60
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 64
A security analyst is reviewing the following event timeline from an COR solution:

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

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

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

Answer: C

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

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

NEW QUESTION 67
A security professional is investigating a trend in vulnerability findings for newly deployed cloud systems Given the following output:

Date	IP address	System name	Finding	Criticality rating
10/13/2023	10.123.34.90	System1	OpenSSL version 1.01	Medium
10/13/2023	10.3.114.72	System6	OpenSSL version 1.01	Medium
10/13/2023	10.12.134.45	System12	Java 11 runtime environment found	Medium
10/13/2023	10.60.65.11	System36	OpenSSL version 1.01	Medium
10/13/2023	10.23.74.9	System37	Java 11 runtime environment found	Medium
10/13/2023	10.13.124.3	System45	OpenSSL version 1.01	Medium

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

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

Answer: A

Explanation:
The output shows that multiple systems have outdated or vulnerable software versions (OpenSSL 1.01 and Java 11 runtime). This suggests that the systems are not being patched regularly or effectively.
? A. Automating the patching system to update base images: Automating the
patching process ensures that the latest security updates and patches are applied to all systems, including newly deployed ones. This addresses the root cause by ensuring that base images used for deployment are always up-to-date with the latest security patches.
? B. Recompiling the affected programs with the most current patches: While this
can fix the immediate vulnerabilities, it does not address the root cause of the problem, which is the lack of regular updates.
? C. Disabling unused/unneeded ports on all servers: This improves security but does not address the specific issue of outdated software.
? D. Deploying a WAF with virtual patching upstream of the affected systems: This can provide a temporary shield but does not resolve the underlying issue of outdated software.
Automating the patching system to update base images ensures that all deployed systems are using the latest, most secure versions of software, addressing the root cause of the vulnerability trend.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-40 Rev. 3, "Guide to Enterprise Patch Management Technologies"
? CIS Controls, "Control 7: Continuous Vulnerability Management"

NEW QUESTION 72
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"

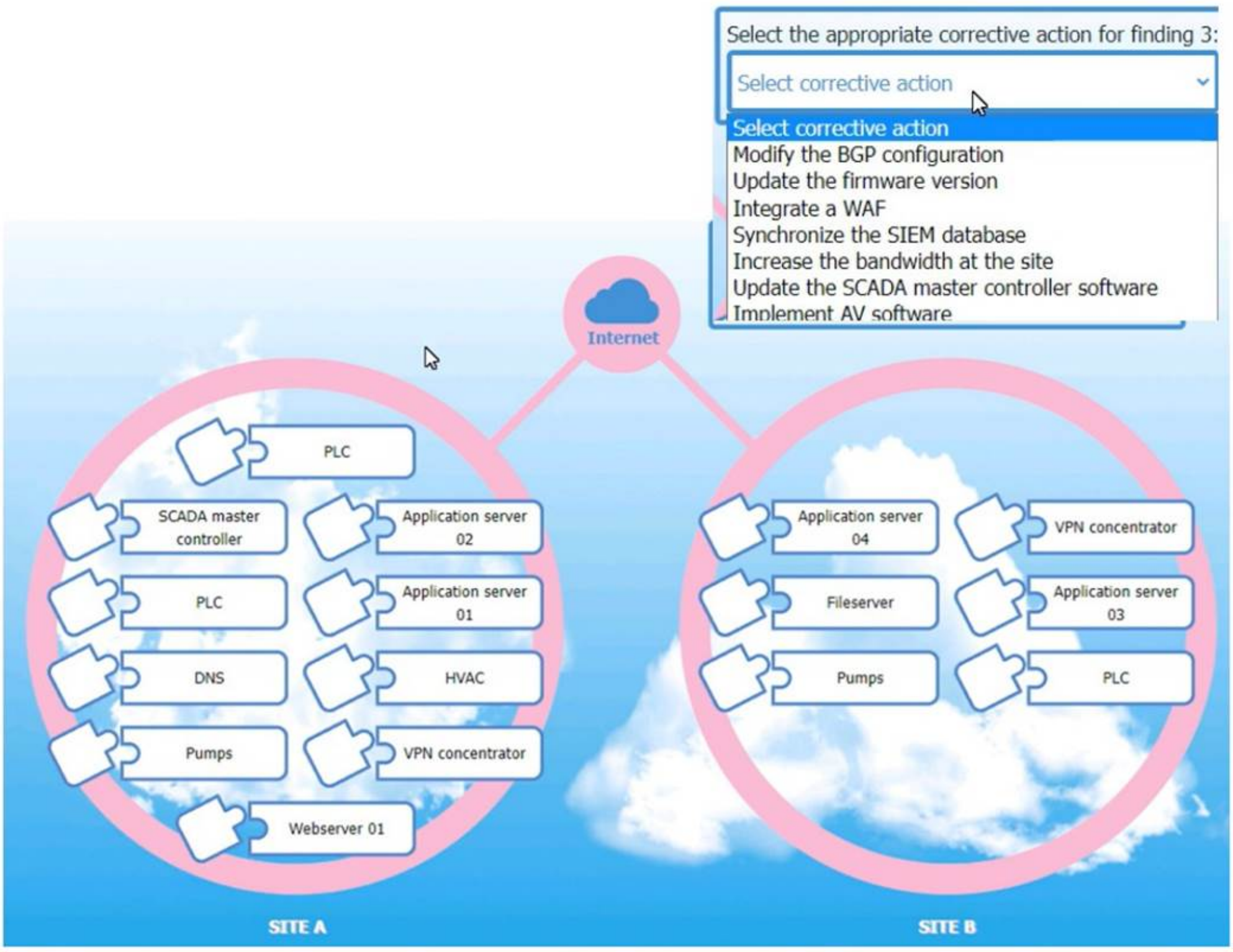
NEW QUESTION 75
SIMULATION
An organization is planning for disaster recovery and continuity of operations, and has noted the following relevant findings:
* 1. A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are
unable to log into the domain from-their 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.



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.

   Select this for the item that should be replicated 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.

   Select this for the item that should be replicated to Site B.

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

   Select this for the item requiring configuration changes.

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 76
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 77
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 81
A cybersecurity architect is reviewing the detection and monitoring capabilities for a global company that recently made multiple acquisitions. The architect discovers that the acquired companies use different vendors for detection and monitoring The architect's goal is to:
• Create a collection of use cases to help detect known threats
• Include those use cases in a centralized library for use across all of the companies Which of the following is the best way to achieve this goal?

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

Answer: A

Explanation:
To create a collection of use cases for detecting known threats and include them in a centralized library for use across multiple companies with different vendors, Sigma rules are the best option. Here??s why:
? Vendor-Agnostic Format: Sigma rules are a generic and open standard for writing
SIEM (Security Information and Event Management) rules. They can be translated to specific query languages of different SIEM systems, making them highly versatile and applicable across various platforms.
? Centralized Rule Management: By using Sigma rules, the cybersecurity architect
can create a centralized library of detection rules that can be easily shared and implemented across different detection and monitoring systems used by the acquired companies. This ensures consistency in threat detection capabilities.
? Ease of Use and Flexibility: Sigma provides a structured and straightforward
format for defining detection logic. It allows for the easy creation, modification, and sharing of rules, facilitating collaboration and standardization across the organization.

NEW QUESTION 83
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 88
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 89
A security engineer wants to reduce the attack surface of a public-facing containerized application Which of the following will best reduce the application's privilege escalation attack surface?

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

Answer: A

Explanation:
Implementing the given commands in the Dockerfile ensures that the container runs with non-root user privileges. Running applications as a non-root user reduces the risk of
privilege escalation attacks because even if an attacker compromises the application, they would have limited privileges and would not be able to perform actions that require root access.
? A. Implementing the following commands in the Dockerfile: This directly addresses
the privilege escalation attack surface by ensuring the application does not run with elevated privileges.
? B. Installing an EDR on the container's host: While useful for detecting threats, this
does not reduce the privilege escalation attack surface within the containerized application.
? C. Designing a multi-container solution: While beneficial for modularity and
remediation, it does not specifically address privilege escalation.
? D. Running the container in an isolated network: This improves network security but does not directly reduce the privilege escalation attack surface.
References:
? CompTIA Security+ Study Guide
? Docker documentation on security best practices
? NIST SP 800-190, "Application Container Security Guide"

NEW QUESTION 90
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 93
A senior security engineer flags me following log file snippet as hawing likely facilitated an attacker's lateral movement in a recent breach:

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

Which of the following solutions, if implemented, would mitigate the nsk of this issue reoccurnnp?

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

Answer: A

Explanation:
The log snippet indicates a DNS AXFR (zone transfer) request, which can be exploited by attackers to gather detailed information about an internal network's infrastructure. Disabling DNS zone transfers is the best solution to mitigate this risk. Zone transfers should generally be restricted to authorized secondary DNS servers and not be publicly accessible, as they can reveal sensitive network information that facilitates lateral movement during an attack.
References:
? CompTIA SecurityX Study Guide: Discusses the importance of securing DNS configurations, including restricting zone transfers.
? NIST Special Publication 800-81, "Secure Domain Name System (DNS) Deployment Guide": Recommends restricting or disabling DNS zone transfers to prevent information leakage.

NEW QUESTION 97
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 98
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 102
A software engineer is creating a CI/CD pipeline to support the development of a web application The DevSecOps team is required to identify syntax errors Which of the following is the most relevant to the DevSecOps team's task'

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

Answer: A

Explanation:
Static Application Security Testing (SAST) involves analyzing source code or compiled code for security vulnerabilities without executing the program. This method is well-suited for identifying syntax errors, coding standards violations, and potential security issues early in the development lifecycle.
? A. Static application security testing (SAST): SAST tools analyze the source code
to detect syntax errors, vulnerabilities, and other issues before the code is run. This is the most relevant task for the DevSecOps team to identify syntax errors and improve code quality.
? B. Software composition analysis: This focuses on identifying vulnerabilities in
open-source components and libraries used in the application but does not address syntax errors directly.
? C. Runtime application self-protection (RASP): RASP involves monitoring and
protecting applications during runtime, which does not help in identifying syntax errors during the development phase.
? D. Web application vulnerability scanning: This involves scanning the running
application for vulnerabilities but does not address syntax errors in the code.
References:
? CompTIA Security+ Study Guide
? OWASP (Open Web Application Security Project) guidelines on SAST
? NIST SP 800-95, "Guide to Secure Web Services" Top of Form
Bottom of Form

NEW QUESTION 105
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 109
A software company deployed a new application based on its internal code repository Several customers are reporting anti-malware alerts on workstations used to test the application Which of the following is the most likely cause of the alerts?

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

Answer: B

Explanation:
The most likely cause of the anti-malware alerts on customer workstations is unsecure bundled libraries. When developing and deploying new applications, it is common for developers to use third-party libraries. If these libraries are not properly vetted for security, they can introduce vulnerabilities or malicious code.
Why Unsecure Bundled Libraries?
? Third-Party Risks: Using libraries that are not secure can lead to malware infections if the libraries contain malicious code or vulnerabilities.
? Code Dependencies: Libraries may have dependencies that are not secure, leading to potential security risks.
? Common Issue: This is a frequent issue in software development where libraries are used for convenience but not properly vetted for security.
Other options, while relevant, are less likely to cause widespread anti-malware alerts:
? A. Misconfigured code commit: Could lead to issues but less likely to trigger anti- malware alerts.
? C. Invalid code signing certificate: Would lead to trust issues but not typically anti- malware alerts.
? D. Data leakage: Relevant for privacy concerns but not directly related to anti- malware alerts.
References:
? CompTIA SecurityX Study Guide
? "Securing Open Source Libraries," OWASP
? "Managing Third-Party Software Security Risks," Gartner Research

NEW QUESTION 110
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 114
A user reports application access issues to the help desk. The help desk reviews the logs for the user

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

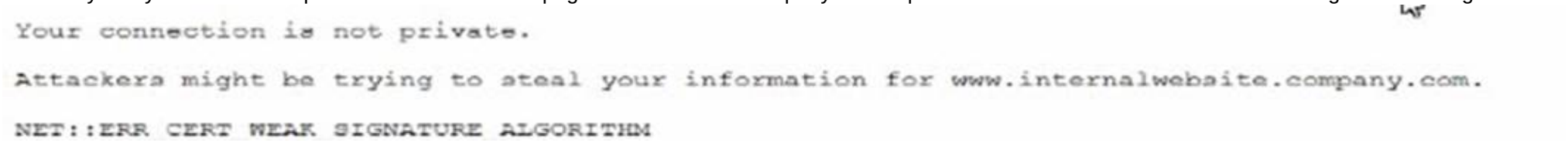
Which of the following is most likely The reason for the issue?

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

Answer: A

Explanation:
Based on the provided logs, the user has accessed various applications from different geographic locations within a very short timeframe. This pattern is indicative of the "impossible travel" security rule, a common feature in Single Sign-On (SSO) systems designed to detect and prevent fraudulent access attempts.
Analysis of Logs:
? At 8:47 p.m., the user accessed a VPN from Toronto.
? At 8:48 p.m., the user accessed email from Los Angeles.
? At 8:48 p.m., the user accessed the human resources system from Los Angeles.
? At 8:49 p.m., the user accessed email again from Los Angeles.
? At 8:52 p.m., the user attempted to access the human resources system from Toronto, which was denied.
These rapid changes in location are physically impossible and typically trigger security measures to prevent unauthorized access. The SSO system detected these inconsistencies and likely flagged the activity as suspicious, resulting in access denial. References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-63B, "Digital Identity Guidelines"
? "Impossible Travel Detection," Microsoft Documentation

NEW QUESTION 117
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 122
.....

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