CompTIA

Exam Questions CAS-005

CompTIA SecurityX Exam

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

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

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

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

Answer: C

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

NEW QUESTION 2
After some employees were caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation. Which of the following would the company most likely do to decrease this type of risk?

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

Answer: B

Explanation:
A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Implementing a CASB provides several benefits:
? A. Improve firewall rules to avoid access to those platforms: This can help but is not as effective or comprehensive as a CASB.
? B. Implement a cloud-access security broker: A CASB can provide visibility into cloud application usage, enforce data security policies, and protect against data leaks by monitoring and controlling access to cloud services. It also provides advanced features like data encryption, data loss prevention (DLP), and compliance monitoring.
? C. Create SIEM rules to raise alerts for access to those platforms: This helps in
monitoring but does not prevent data leaks.
? D. Deploy an internet proxy that filters certain domains: This can block access to specific sites but lacks the granular control and visibility provided by a CASB.
Implementing a CASB is the most comprehensive solution to decrease the risk of data leaks by providing visibility, control, and enforcement of security policies for cloud services. References:
? CompTIA Security+ Study Guide
? Gartner, "Magic Quadrant for Cloud Access Security Brokers"
? NIST SP 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"

NEW QUESTION 3
Within a SCADA a business needs access to the historian server in order together metric about the functionality of the environment. Which of the following actions should be taken to address this requirement?

A. Isolating the historian server for connections only from The SCADA environment
B. Publishing the C$ share from SCADA to the enterprise
C. Deploying a screened subnet between 11 and SCADA
D. Adding the business workstations to the SCADA domain

Answer: A

Explanation:
The best action to address the requirement of accessing the historian server within a SCADA system is to isolate the historian server for connections only from the SCADA environment. Here??s why:
? Security and Isolation: Isolating the historian server ensures that only authorized
devices within the SCADA environment can connect to it. This minimizes the attack surface and protects sensitive data from unauthorized access.
? Access Control: By restricting access to the historian server to only SCADA
devices, the organization can better control and monitor interactions, ensuring that only legitimate queries and data retrievals occur.
? Best Practices for Critical Infrastructure: Following the principle of least privilege,
isolating critical components like the historian server is a standard practice in securing SCADA systems, reducing the risk of cyberattacks.
? References:

NEW QUESTION 4
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 5
A global manufacturing company has an internal application mat is critical to making products This application cannot be updated and must Be available in the production area A security architect is implementing security for the application. Which of the following best describes the action the architect should take-?

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

Answer: D

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

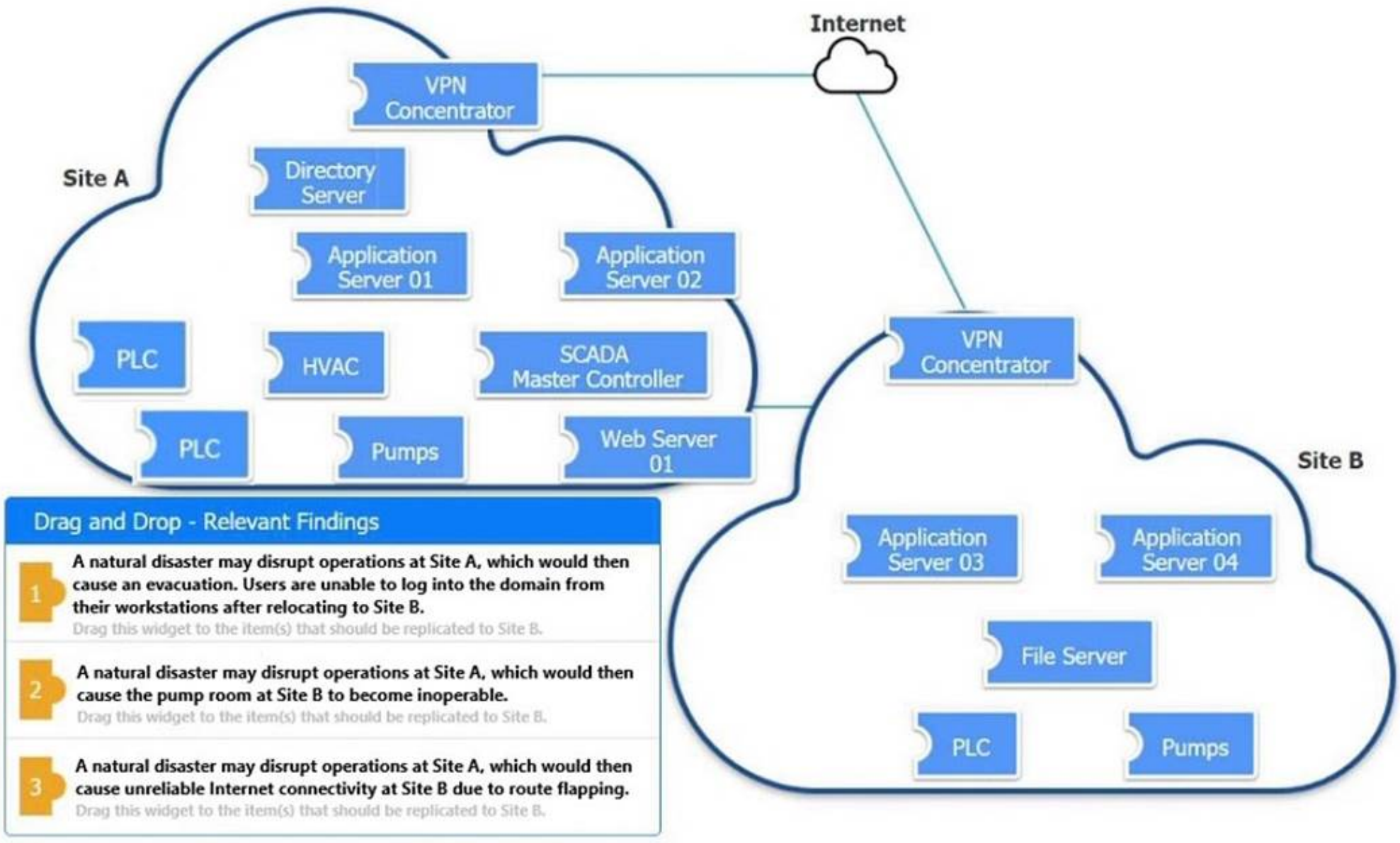
NEW QUESTION 6
A user submits a help desk ticket stating then account does not authenticate sometimes. An analyst reviews the following logs for the user:
Which of the following best explains the reason the user's access is being denied?

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

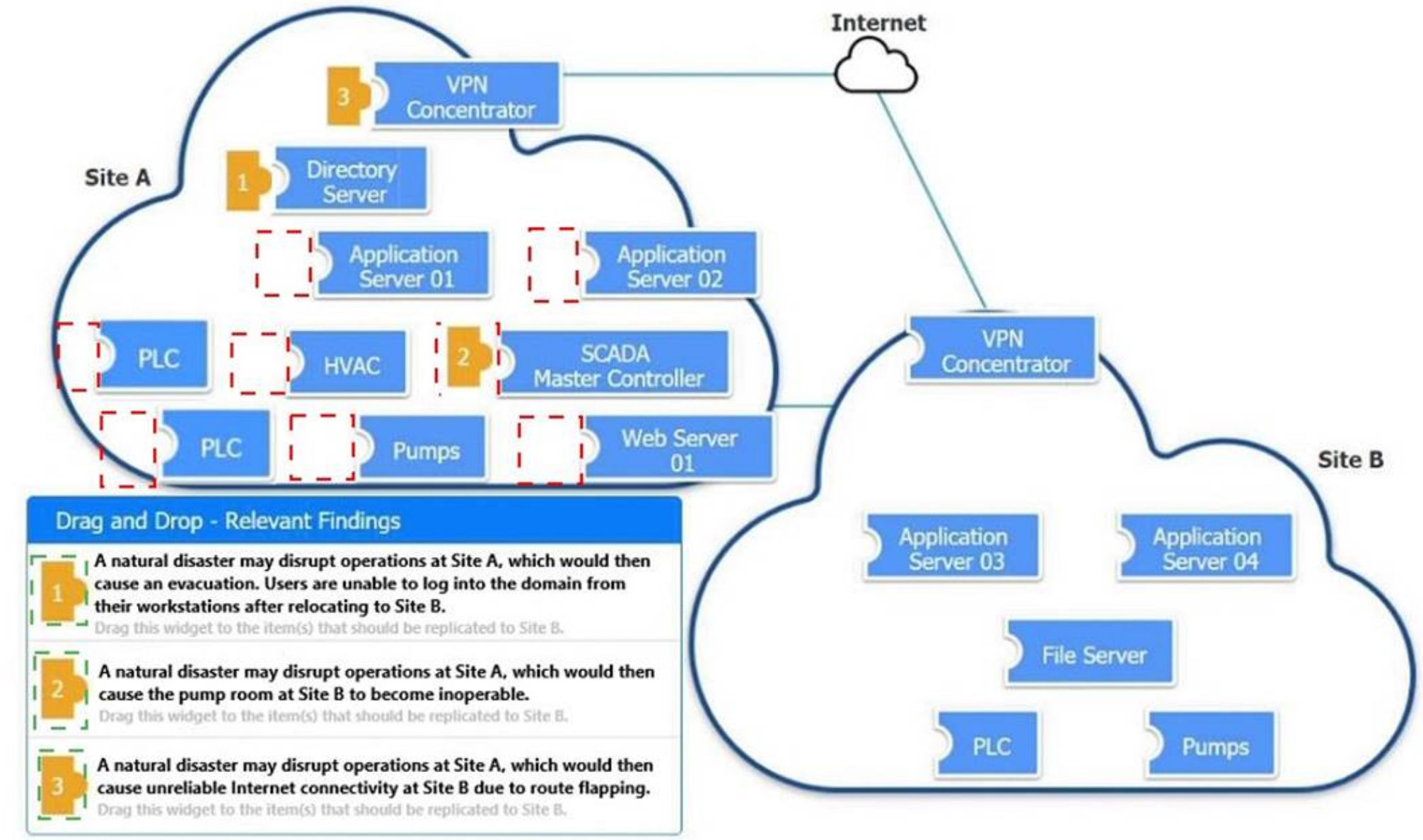
Answer: B

Explanation:
The logs reviewed for the user indicate that access is being denied due to time-based access restrictions. These restrictions are commonly implemented to limit access to systems during specific hours to enhance security. If a user attempts to authenticate outside of the allowed time window, access will be denied. This measure helps prevent unauthorized access during non-business hours, reducing the risk of security incidents.
References:
? CompTIA SecurityX Study Guide: Covers various access control methods, including time-based restrictions, as a means of enhancing security.
? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations": Recommends the use of time-based access restrictions as part of access control policies.
? "Access Control and Identity Management" by Mike Chapple and Aaron French: Discusses the implementation and benefits of time-based access restrictions.

NEW QUESTION 7
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 8
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 9
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 10
A security analyst is reviewing the following authentication logs:

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

Which of the following should the analyst do first?

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

Answer: D

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

NEW QUESTION 10
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 15
Company A and Company D ate merging Company A's compliance reports indicate branch protections are not in place A security analyst needs to ensure that potential threats to the software development life cycle are addressed. Which of the following should me analyst cons<der when completing this basic?

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

Answer: C

Explanation:
Dynamic Application Security Testing (DAST) is crucial for identifying and addressing security vulnerabilities during the software development life cycle (SDLC). Ensuring that DAST scans are routinely scheduled helps in maintaining a secure development process. Why Routine DAST Scans?
? Continuous Security Assessment: Regular DAST scans help in identifying vulnerabilities in real-time, ensuring they are addressed promptly.
? Compliance: Routine scans ensure that the development process complies with security standards and regulations.
? Proactive Threat Mitigation: Regular scans help in early detection and mitigation of potential security threats, reducing the risk of breaches.
? Integration into SDLC: Ensures security is embedded within the development process, promoting a security-first approach.
Other options, while relevant, do not directly address the continuous assessment and proactive identification of threats:
? A. If developers are unable to promote to production: This is more of an operational issue than a security assessment.
? B. If DAST code is being stored to a single code repository: This concerns code management rather than security testing frequency.
? D. If role-based training is deployed: While important, training alone does not ensure continuous security assessment.
References:
? CompTIA SecurityX Study Guide
? OWASP Testing Guide
? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations"

NEW QUESTION 16
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 17
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

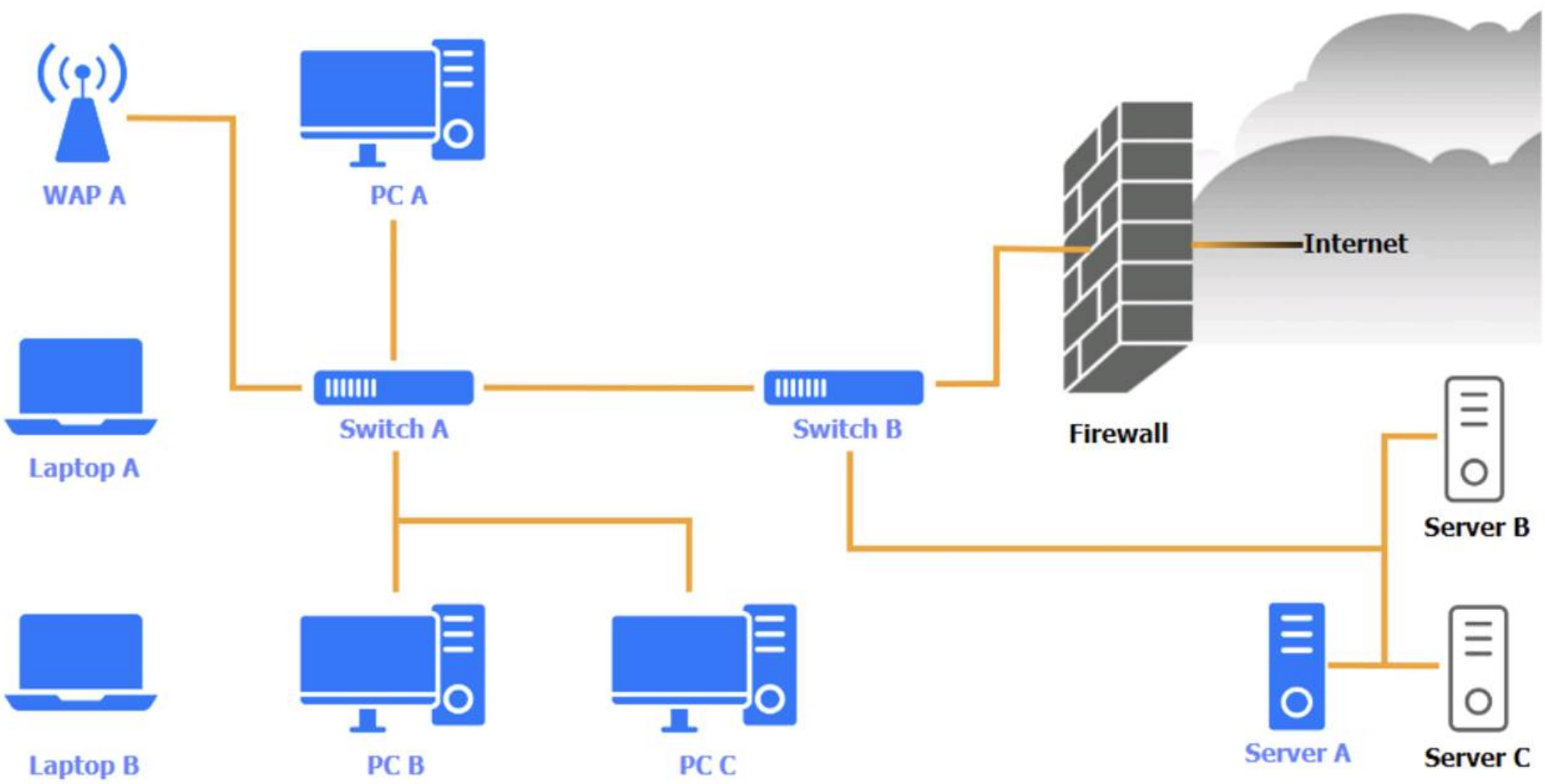
NEW QUESTION 19
Users are experiencing a variety of issues when trying to access corporate resources examples include
• Connectivity issues between local computers and file servers within branch offices
• Inability to download corporate applications on mobile endpoints wtiilc working remotely
• Certificate errors when accessing internal web applications
Which of the following actions are the most relevant when troubleshooting the reported issues? (Select two).

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

Answer: AF

Explanation:
The reported issues suggest problems related to network connectivity, remote access, and certificate management:
? A. Review VPN throughput: Connectivity issues and the inability to download applications while working remotely may be due to VPN bandwidth or performance issues. Reviewing and optimizing VPN throughput can help resolve these problems by ensuring that remote users have adequate bandwidth for accessing corporate resources.
? F. Validate MDM asset compliance: Mobile Device Management (MDM) systems ensure that mobile endpoints comply with corporate security policies. Validating MDM compliance can help address issues related to the inability to download applications and certificate errors, as non-compliant devices might be blocked from accessing certain resources.
? B. Check IPS rules: While important for security, IPS rules are less likely to directly address the connectivity and certificate issues described.
? C. Restore static content on the CDN: This action is related to content delivery but does not address VPN or certificate-related issues.
? D. Enable secure authentication using NAC: Network Access Control (NAC) enhances security but does not directly address the specific issues described.
? E. Implement advanced WAF rules: Web Application Firewalls protect web applications but do not address VPN throughput or mobile device compliance.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-77, "Guide to IPsec VPNs"
? CIS Controls, "Control 11: Secure Configuration for Network Devices"

NEW QUESTION 23
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

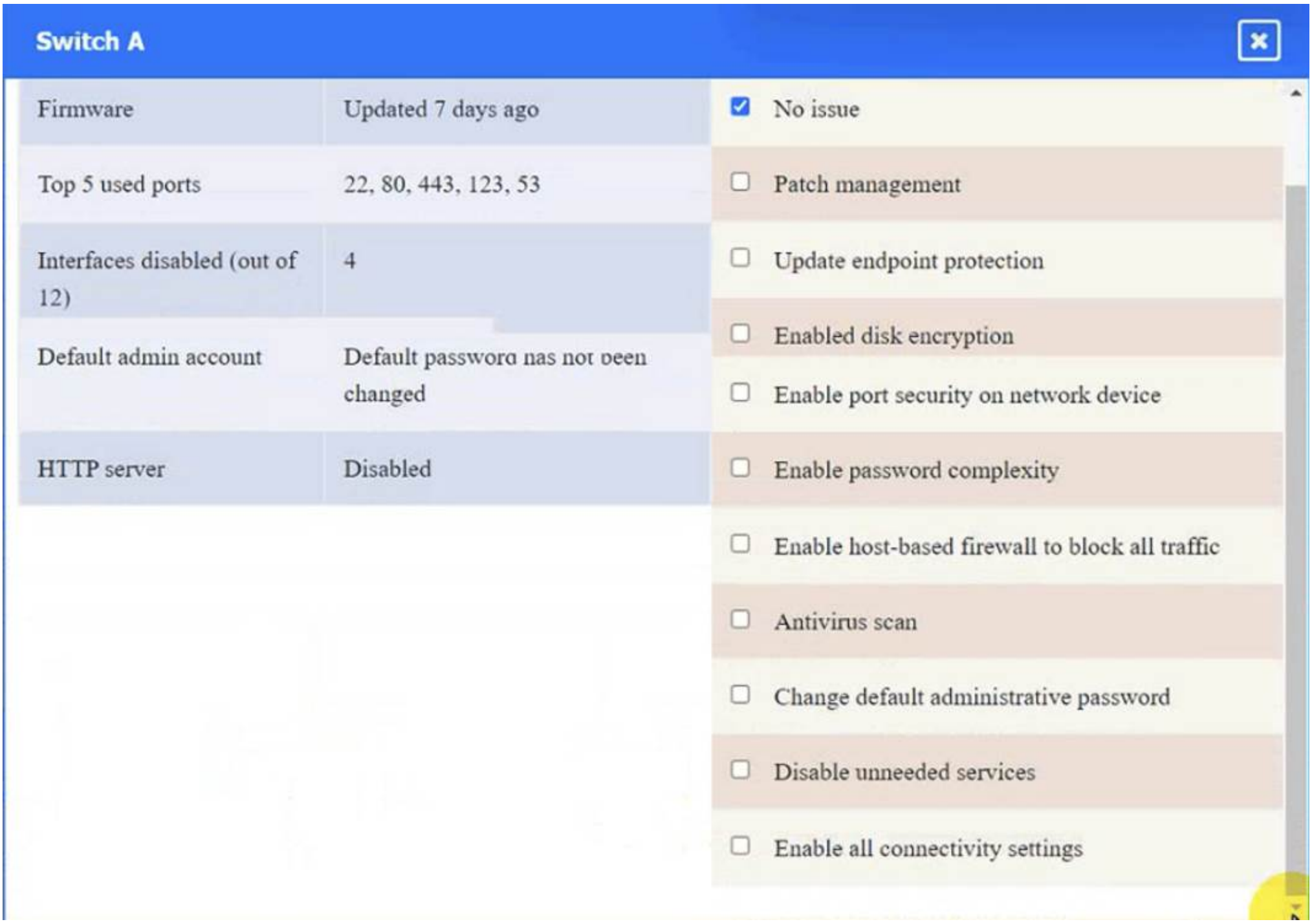
Laptop A

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

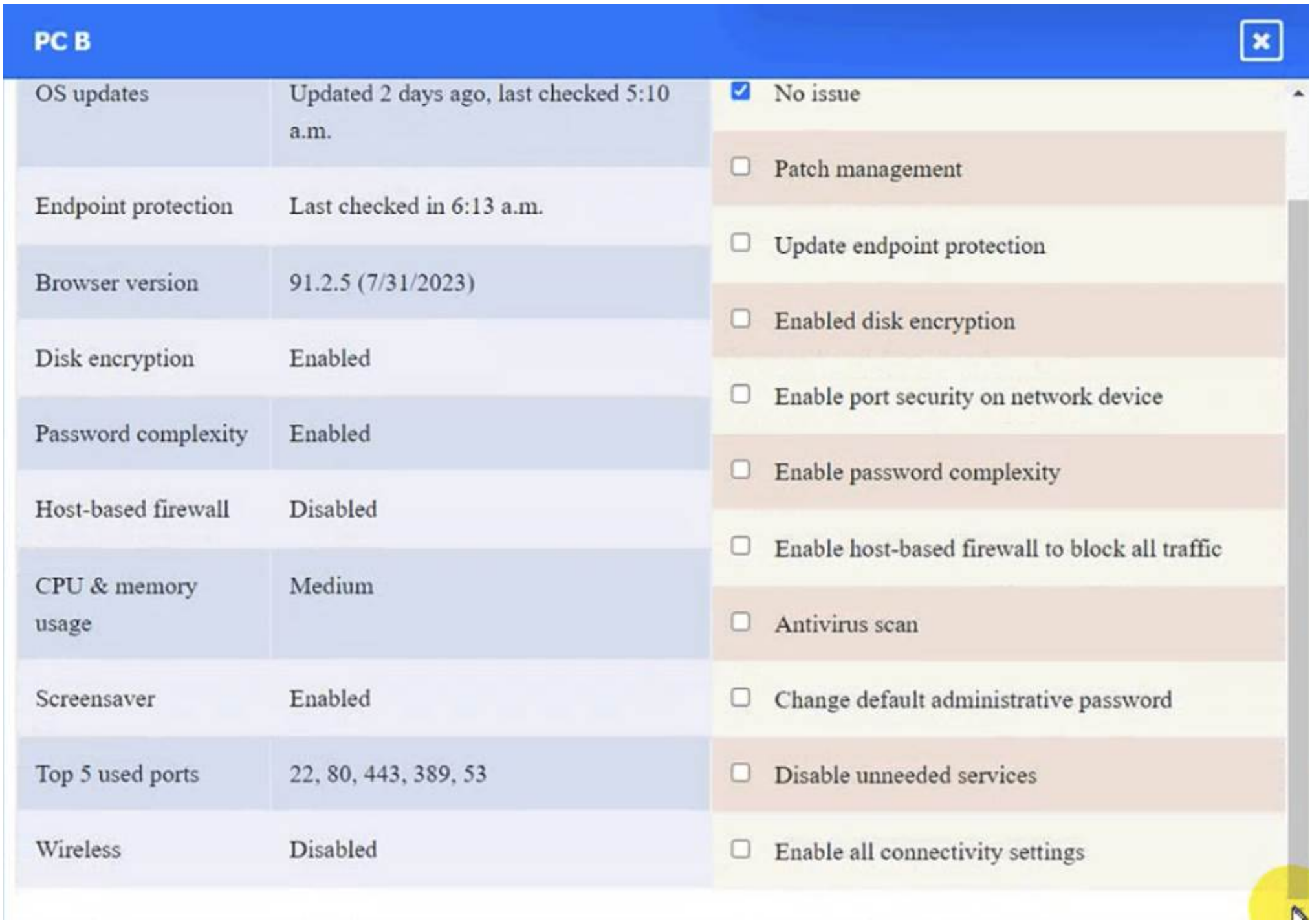
Firmware	Updated 7 days ago	☑ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
Interfaces disabled (out of 6)	1	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
		☐ Enable port security on network device
HTTP server	Disabled	☐ 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

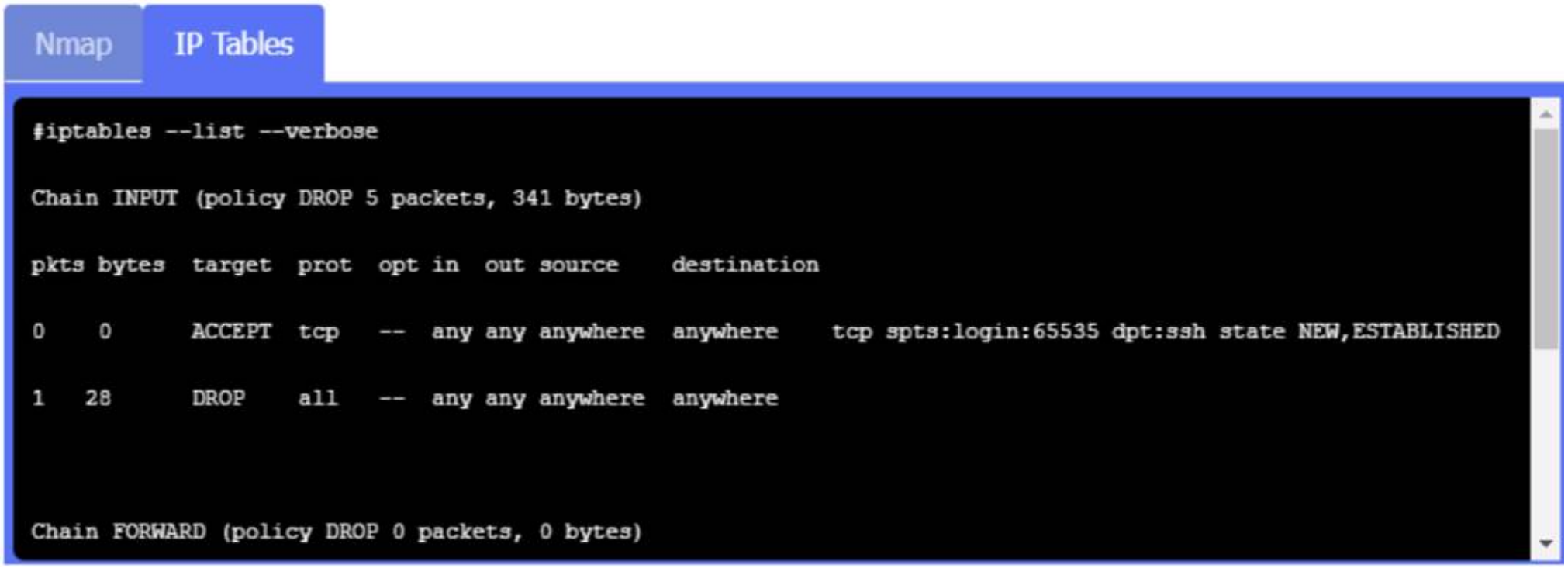
```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

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

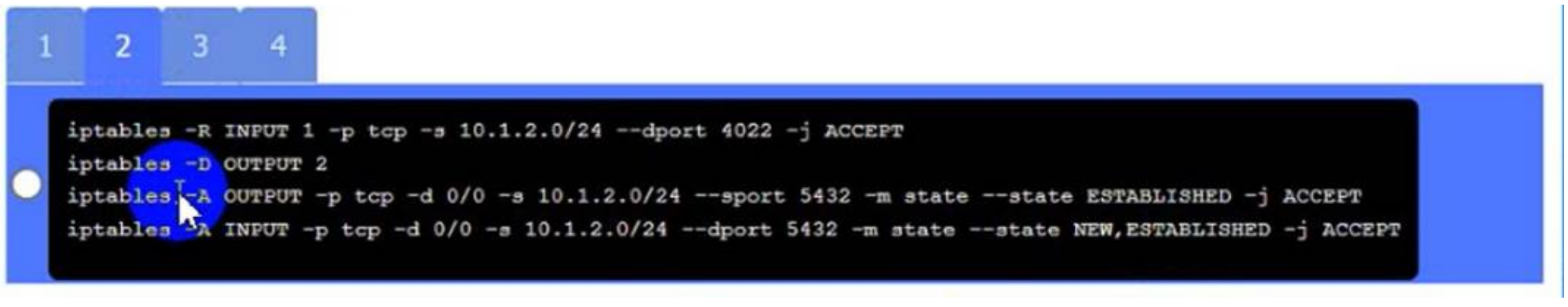
```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --dport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```



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 27
A company receives reports about misconfigurations and vulnerabilities in a third-party hardware device that is part of its released products. Which of the following solutions is the best way for the company to identify possible issues at an earlier stage?

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

Answer: D

Explanation:
Addressing misconfigurations and vulnerabilities in third-party hardware requires a comprehensive approach to manage risks throughout the supply chain. Implementing a proper supply chain risk management (SCRM) program is the most effective solution as it encompasses the following:
? Holistic Approach: SCRM considers the entire lifecycle of the product, from initial
design through to delivery and deployment. This ensures that risks are identified and managed at every stage.
? Vendor Management: It includes thorough vetting of suppliers and ongoing
assessments of their security practices, which can identify and mitigate vulnerabilities early.
? Regular Audits and Assessments: A robust SCRM program involves regular audits
and assessments, both internally and with suppliers, to ensure compliance with security standards and best practices.
? Collaboration and Communication: Ensures that there is effective communication
and collaboration between the company and its suppliers, leading to faster identification and resolution of issues.
Other options, while beneficial, do not provide the same comprehensive risk management:
? A. Performing vulnerability tests on each device delivered by the providers: While useful, this is reactive and only addresses issues after they have been delivered.
? B. Performing regular red-team exercises on the vendor production line: This can identify vulnerabilities but is not as comprehensive as a full SCRM program.
? C. Implementing a monitoring process for the integration between the application and the vendor appliance: This is important but only covers the integration phase, not the entire supply chain.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"
? ISO/IEC 27036-1:2014, "Information technology — Security techniques — Information security for supplier relationships"

NEW QUESTION 32
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 36
A company that uses containers to run its applications is required to identify vulnerabilities on every container image in a private repository The security team needs to be able to quickly evaluate whether to respond to a given vulnerability Which of the following, will allow the security team to achieve the objective with the last effort?

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

Answer: B

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

NEW QUESTION 40
A company wants to invest in research capabilities with the goal to operationalize the research output. Which of the following is the best option for a security architect to recommend?

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

Answer: B

Explanation:
Investing in a threat intelligence platform is the best option for a company looking to operationalize research output. A threat intelligence platform helps in collecting, processing, and analyzing threat data to provide actionable insights. These platforms integrate data from various sources, including dark web monitoring, honeypots, and other security tools, to offer a comprehensive view of the threat landscape.
Why a Threat Intelligence Platform?
? Data Integration: It consolidates data from multiple sources, including dark web monitoring and honeypots, making it easier to analyze and derive actionable insights.
? Actionable Insights: Provides real-time alerts and reports on potential threats, helping the organization take proactive measures.
? Operational Efficiency: Streamlines the process of threat detection and response, allowing the security team to focus on critical issues.
? Research and Development: Facilitates the operationalization of research output by providing a platform for continuous monitoring and analysis of emerging threats.
Other options, while valuable, do not offer the same level of integration and operationalization capabilities:
? A. Dark web monitoring: Useful for specific threat intelligence but lacks
comprehensive operationalization.
? C. Honeypots: Effective for detecting and analyzing specific attack vectors but not for broader threat intelligence.
? D. Continuous adversary emulation: Important for testing defenses but not for integrating and operationalizing threat intelligence.
References:
? CompTIA SecurityX Study Guide
? "Threat Intelligence Platforms," Gartner Research
? NIST Special Publication 800-150, "Guide to Cyber Threat Information Sharing"

NEW QUESTION 42
Audit findings indicate several user endpoints are not utilizing full disk encryption During me remediation process, a compliance analyst reviews the testing details for the endpoints and notes the endpoint device configuration does not support full disk encryption Which of the following is the most likely reason me device must be replaced'

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

Answer: D

Explanation:
The most likely reason the device must be replaced is that the motherboard was not configured with a TPM (Trusted Platform Module) from the OEM (Original Equipment Manufacturer) supplier.
Why TPM is Necessary for Full Disk Encryption:
? Hardware-Based Security: TPM provides a hardware-based mechanism to store encryption keys securely, which is essential for full disk encryption.
? Compatibility: Full disk encryption solutions, such as BitLocker, require TPM to ensure that the encryption keys are securely stored and managed.
? Integrity Checks: TPM enables system integrity checks during boot, ensuring that the device has not been tampered with.
Other options do not directly address the requirement for TPM in supporting full disk encryption:
? A. The HSM is outdated: While HSM (Hardware Security Module) is important for
security, it is not typically used for full disk encryption.
? B. The vTPM was not properly initialized: vTPM (virtual TPM) is less common and not typically a reason for requiring hardware replacement.
? C. The HSM is vulnerable to common exploits: This would require a firmware upgrade, not replacement of the device.
? E. The HSM does not support sealing storage: Sealing storage is relevant but not the primary reason for requiring TPM for full disk encryption.
References:
? CompTIA SecurityX Study Guide
? "Trusted Platform Module (TPM) Overview," Microsoft Documentation
? "BitLocker Deployment Guide," Microsoft Documentation

NEW QUESTION 44
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 49
A systems administrator wants to use existing resources to automate reporting from disparate security appliances that do not currently communicate. Which of the following is the best way to meet this objective?

A. Configuring an API Integration to aggregate the different data sets
B. Combining back-end application storage into a single, relational database
C. Purchasing and deploying commercial off the shelf aggregation software
D. Migrating application usage logs to on-premises storage

Answer: A

Explanation:
The best way to automate reporting from disparate security appliances that do not currently communicate is to configure an API Integration to aggregate the different data sets. Here's why:
? Interoperability: APIs allow different systems to communicate and share data, even
if they were not originally designed to work together. This enables the integration of various security appliances into a unified reporting system.
? Automation: API integrations can automate the process of data collection,
aggregation, and reporting, reducing manual effort and increasing efficiency.
? Scalability: APIs provide a scalable solution that can easily be extended to include
additional security appliances or data sources as needed.
? References:

NEW QUESTION 51
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 55
A financial services organization is using Al lo fully automate the process of deciding client loan rates Which of the following should the organization be most concerned about from a privacy perspective?

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

Answer: A

Explanation:
When using AI to fully automate the process of deciding client loan rates, the primary concern from a privacy perspective is model explainability.
Why Model Explainability is Critical:
? Transparency: It ensures that the decision-making process of the AI model can be understood and explained to stakeholders, including clients.
? Accountability: Helps in identifying biases and errors in the model, ensuring that the AI is making fair and unbiased decisions.
? Regulatory Compliance: Various regulations require that decisions, especially those affecting individuals' financial status, can be explained and justified.
? Trust: Builds trust among users and stakeholders by demonstrating that the AI decisions are transparent and justifiable.
Other options, such as credential theft, prompt injections, and social engineering, are significant concerns but do not directly address the privacy and fairness implications of automated decision-making.
References:
? CompTIA SecurityX Study Guide
? "The Importance of Explainability in AI," IEEE Xplore
? GDPR Article 22, "Automated Individual Decision-Making, Including Profiling"

NEW QUESTION 56
An organization is required to
* Respond to internal and external inquiries in a timely manner
* Provide transparency.
* Comply with regulatory requirements
The organization has not experienced any reportable breaches but wants to be prepared if a breach occurs in the future. Which of the following is the best way for the organization to prepare?

A. Outsourcing the handling of necessary regulatory filing to an external consultant
B. Integrating automated response mechanisms into the data subject access request process
C. Developing communication templates that have been vetted by internal and external counsel

D. Conducting lessons-learned activities and integrating observations into the crisis management plan

Answer: C

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

NEW QUESTION 57
A vulnerability can on a web server identified the following:

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

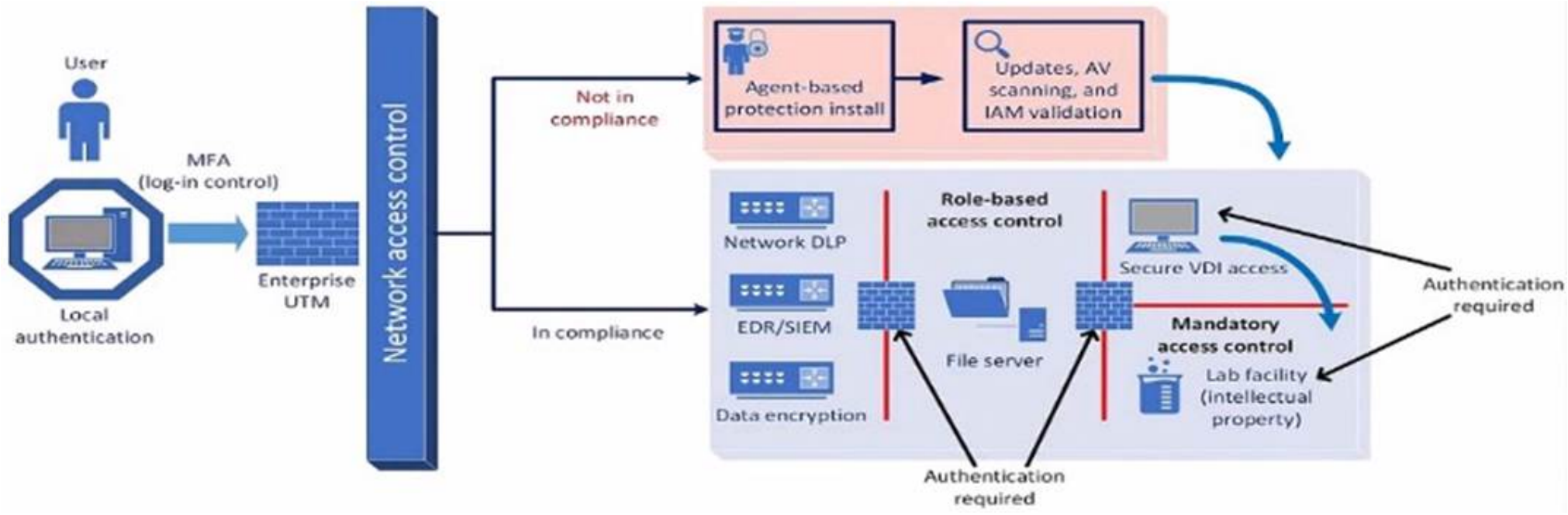
Which of the following actions would most likely eliminate on path decryption attacks? (Select two).

A. Disallowing cipher suites that use ephemeral modes of operation for key agreement
B. Removing support for CBC-based key exchange and signing algorithms
C. Adding TLS_ECDHE_ECDSA_WITH_AE3_256_GCMS_HA256
D. Implementing HIPS rules to identify and block BEAST attack attempts
E. Restricting cipher suites to only allow TLS_RSA_WITH_AES_128_CBC_SHA
F. Increasing the key length to 256 for TLS_RSA_WITH_AES_128_CBC_SHA

Answer: BC

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

NEW QUESTION 59
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 60
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 62
A security analyst Detected unusual network traffic related to program updating processes The analyst collected artifacts from compromised user workstations. The discovered artifacts were binary files with the same name as existing, valid binaries but. with different hashes which of the following solutions would most likely prevent this situation from reoccurring?

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

Answer: B

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

NEW QUESTION 66
An organization is implementing Zero Trust architecture A systems administrator must increase the effectiveness of the organization's context-aware access system. Which of the following is the best way to improve the effectiveness of the system?

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

Answer: D

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

NEW QUESTION 69
A security administrator needs to automate alerting. The server generates structured log files that need to be parsed to determine whether an alarm has been triggered Given the following code function:

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

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

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

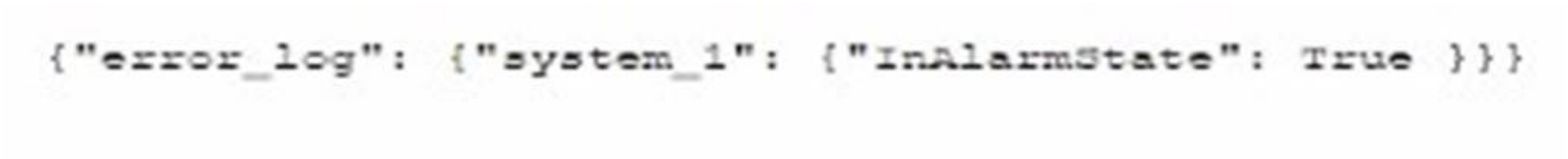
B)

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

C)

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

D)



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

Answer: A

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

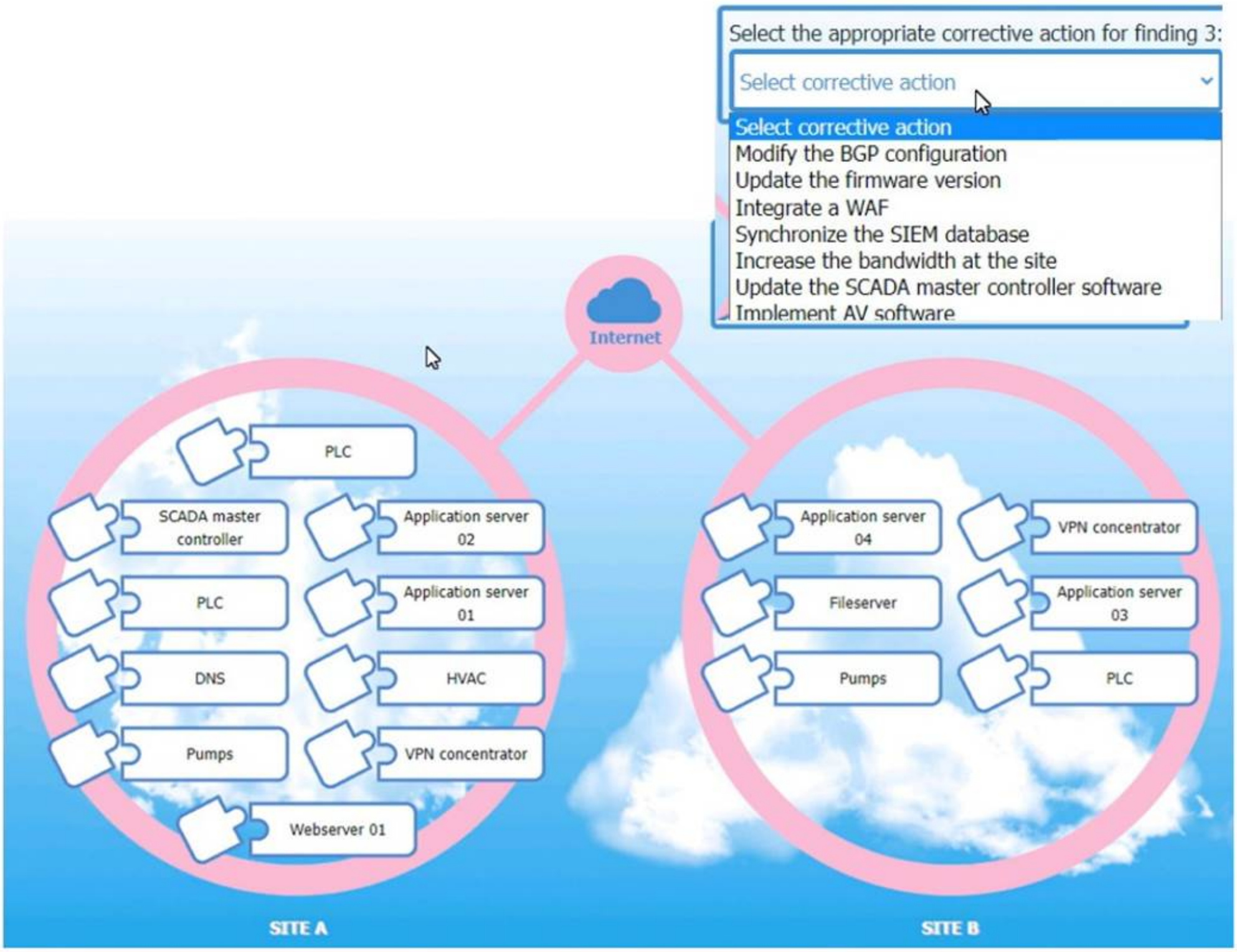
NEW QUESTION 74
A cloud engineer needs to identify appropriate solutions to:
• Provide secure access to internal and external cloud resources.
• Eliminate split-tunnel traffic flows.
• Enable identity and access management capabilities.
Which of the following solutions arc the most appropriate? (Select two).

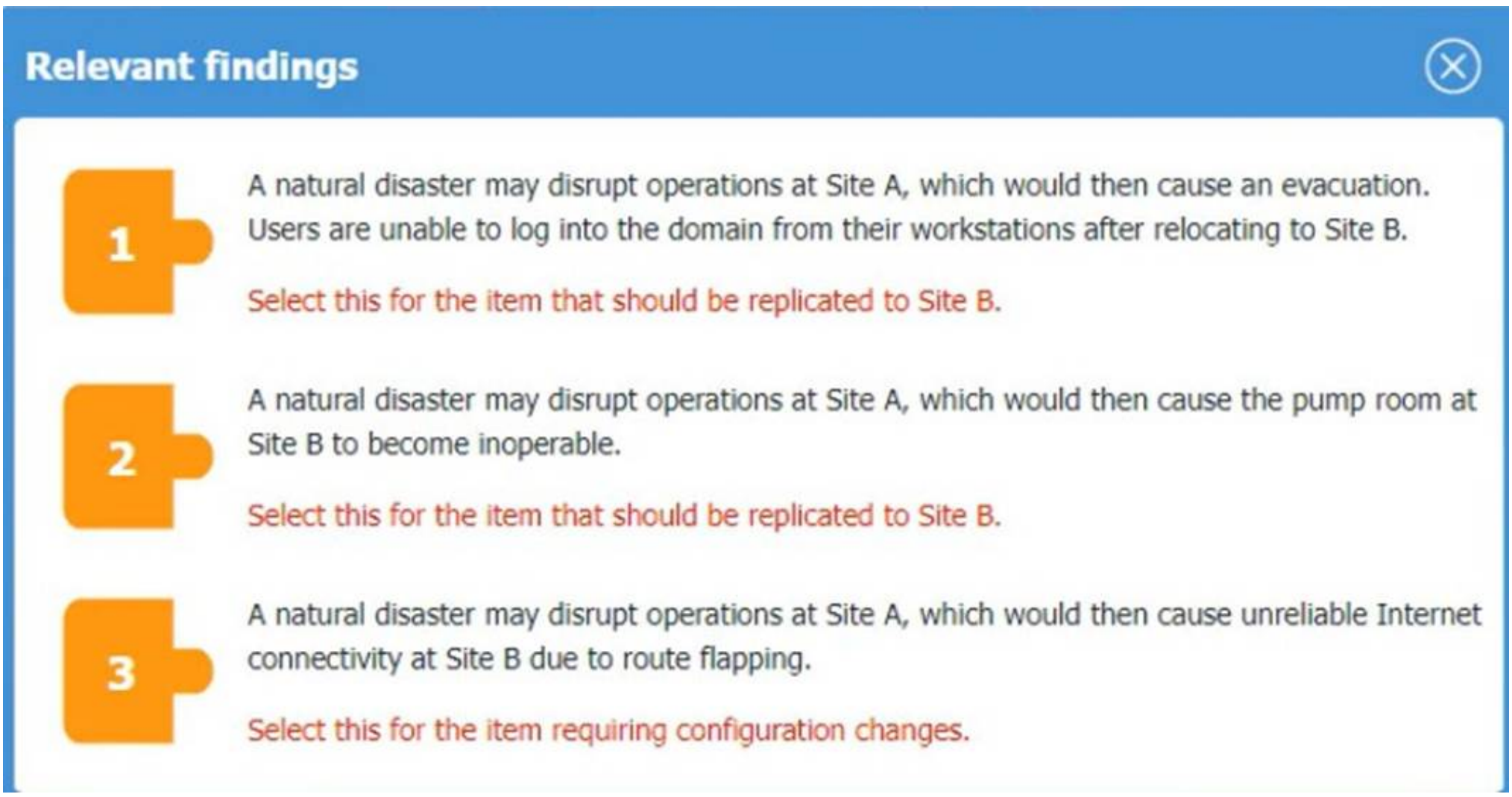
A. Federation
B. Microsegmentation
C. CASB
D. PAM
E. SD-WAN
F. SASE

Answer: CF

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

NEW QUESTION 79
SIMULATION
An organization is planning for disaster recovery and continuity of operations, and has noted the following relevant findings:
* 1. A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from-their workstations after relocating to Site B.
* 2. A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.
* 3. A natural disaster may disrupt operations at Site A, which would then cause unreliable internet connectivity at Site B due to route flapping.
INSTRUCTIONS
Match each relevant finding to the affected host by clicking on the host name and selecting the appropriate number.
For findings 1 and 2, select the items that should be replicated to Site B. For finding 3, select the item requiring configuration changes, then select the appropriate corrective action from the drop-down menu.





A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 82
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 84
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 87
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 92
An organization wants to manage specialized endpoints and needs a solution that provides the ability to
* Centrally manage configurations
* Push policies.
• Remotely wipe devices
• Maintain asset inventory
Which of the following should the organization do to best meet these requirements?

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

Answer: B

Explanation:
To meet the requirements of centrally managing configurations, pushing policies, remotely wiping devices, and maintaining an asset inventory, the best solution is to implement a Mobile Device Management (MDM) solution.
MDM Capabilities:
? Central Management: MDM allows administrators to manage the configurations of all devices from a central console.
? Policy Enforcement: MDM solutions enable the push of security policies and updates to ensure compliance across all managed devices.
? Remote Wipe: In case a device is lost or stolen, MDM provides the capability to remotely wipe the device to protect sensitive data.
? Asset Inventory: MDM maintains an up-to-date inventory of all managed devices, including their configurations and installed applications.
Other options do not provide the same comprehensive capabilities required for managing specialized endpoints.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-124 Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise"
? "Mobile Device Management Overview," Gartner Research

NEW QUESTION 96
A systems administrator wants to reduce the number of failed patch deployments in an organization. The administrator discovers that system owners modify systems or applications in an ad hoc manner. Which of the following is the best way to reduce the number of failed patch deployments?

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

Answer: C

Explanation:
To reduce the number of failed patch deployments, the systems administrator should implement a robust change management process. Change management ensures that all modifications to systems or applications are planned, tested, and approved before deployment. This systematic approach reduces the risk of unplanned changes that can cause patch failures and ensures that patches are deployed in a controlled and predictable manner.
References:
? CompTIA SecurityX Study Guide: Emphasizes the importance of change management in maintaining system integrity and ensuring successful patch deployments.
? ITIL (Information Technology Infrastructure Library) Framework: Provides best practices for change management in IT services.
? "The Phoenix Project" by Gene Kim, Kevin Behr, and George Spafford: Discusses the critical role of change management in IT operations and its impact on system stability and reliability.

NEW QUESTION 100
A hospital provides tablets to its medical staff to enable them to more quickly access and edit patients' charts. The hospital wants to ensure that if a tablet is Identified as lost or stolen and a remote command is issued, the risk of data loss can be mitigated within seconds. The tablets are configured as follows to meet hospital policy
• Full disk encryption is enabled
• "Always On" corporate VPN is enabled
• ef-use-backed keystore is enabled'ready.
• Wi-Fi 6 is configured with SAE.
• Location services is disabled.

•Application allow list is configured

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

Answer: E

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

NEW QUESTION 102
SIMULATION
A product development team has submitted code snippets for review prior to release. INSTRUCTIONS
Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.
Code Snippet 1

Code Snippet 1 | Code Snippet 2

```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103



Web server code:
…
String accountQuery = “SELECT * from users WHERE userid = ?”;
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter(“userid”));
ResultSet queryResponse = stmt.executeQuery();
…
```

Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103


API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5, 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
 userId = request.getParam(userid)

 ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                          -h loginserver.comptia.org
                          -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
...
```

Vulnerability 1:
? SQL injection
? Cross-site request forgery
? Server-side request forgery
? Indirect object reference
? Cross-site scripting
Fix 1:
? Perform input sanitization of the userid field.
? Perform output encoding of queryResponse,
? Ensure usex:ia belongs to logged-in user.
? Inspect URLS and disallow arbitrary requests.
? Implement anti-forgery tokens.
Vulnerability 2
1) Denial of service
2) Command injection
3) SQL injection
4) Authorization bypass
5) Credentials passed via GET
Fix 2
A) Implement prepared statements and bind variables.
B) Remove the serve_forever instruction.
C) Prevent the "authenticated" value from being overridden by a GET parameter.
D) HTTP POST should be used for sensitive parameters.
E) Perform input sanitization of the userid field.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Code Snippet 1
Vulnerability 1: SQL injection
SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.
Fix 1: Perform input sanitization of the userid field.
Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.
Code Snippet 2
Vulnerability 2: Cross-site request forgery
Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.
Fix 2: Implement anti-forgery tokens.
Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user??s browser can be accepted by the server.

NEW QUESTION 106
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 107
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 108
A company lined an email service provider called my-email.com to deliver company emails. The company stalled having several issues during the migration. A security engineer is troubleshooting and observes the following configuration snippet:

@	MX	10	email.company.com	45000
www	IN	CNAME	web01.company.com.	
email	IN	CNAME	srv01.company.com	
srv01	IN	A	192.168.1.10	
web01	IN	A	192.168.1.11	
@	IN	TXT	"v=dmarc include:company.com ~all"	

Which of the following should the security engineer modify to fix the issue? (Select two).

A. The email CNAME record must be changed to a type A record pointing to 192.168.111
B. The TXT record must be Changed to "v=dmarc ip4:192.168.1.10 include:my-email.com - all"
C. The srvo1 A record must be changed to a type CNAME record pointing to the email server
D. The email CNAME record must be changed to a type A record pointing to 192.168.1.10
E. The TXT record must be changed to "v=dkim ip4:l92.168.1.11 include my-email.com - ell"
F. The TXT record must be Changed to "v=dkim ip4:192.168.1.10 include:email-all"

G. The srv01 A record must be changed to a type CNAME record pointing to the web01 server

Answer: BD

Explanation:
The security engineer should modify the following to fix the email migration issues:
? Email CNAME Record: The email CNAME record must be changed to a type A record pointing to 192.168.1.10. This is because CNAME records should not be used where an IP address (A record) is required. Changing it to an A record ensures direct pointing to the correct IP.
? TXT Record for DMARC: The TXT record must be changed to "v=dmarc ip4:192.168.1.10 include
com -all". This ensures proper configuration of DMARC (Domain-based Message Authentication, Reporting & Conformance) to include the correct IP address and the email service provider domain.
? uk.co.certification.simulator.questionpool.PList@488ba0cc
? References:

NEW QUESTION 109
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 112
.....

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