CompTIA

Exam Questions CAS-005

CompTIA SecurityX Exam

NEW QUESTION 1
An organization wants to implement a platform to better identify which specific assets are affected by a given vulnerability. Which of the following components provides the best foundation to achieve this goal?

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

Answer: B

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

NEW QUESTION 2
A developer needs to improve the cryptographic strength of a password-storage component in a web application without completely replacing the crypto-module. Which of the following is the most appropriate technique?

A. Key splitting
B. Key escrow
C. Key rotation
D. Key encryption
E. Key stretching

Answer: E

Explanation:
The most appropriate technique to improve the cryptographic strength of a password-storage component in a web application without completely replacing the crypto- module is key stretching. Here's why:
? Enhanced Security: Key stretching algorithms, such as PBKDF2, bcrypt, and scrypt, increase the computational effort required to derive the encryption key from the password, making brute-force attacks more difficult and time-consuming.
? Compatibility: Key stretching can be implemented alongside existing cryptographic modules, enhancing their security without the need for a complete overhaul.
? Industry Best Practices: Key stretching is a widely recommended practice for securely storing passwords, as it significantly improves resistance to password-cracking attacks.
? References:

NEW QUESTION 3
A news organization wants to implement workflows that allow users to request that untruthful data be retraced and scrubbed from online publications to comply with the right to be forgotten Which of the following regulations is the organization most likely trying to address'

A. GDPR
B. COPPA
C. CCPA
D. DORA

Answer: A

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

NEW QUESTION 4
Users are willing passwords on paper because of the number of passwords needed in an environment. Which of the following solutions is the best way to manage this situation and decrease risks?

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

Answer: B

Explanation:
Implementing a Single Sign-On (SSO) solution and integrating it with applications is the best way to manage the situation and decrease risks. Here??s why:
? Reduced Password Fatigue: SSO allows users to log in once and gain access to multiple applications and systems without needing to remember and manage

multiple passwords. This reduces the likelihood of users writing down passwords.
? Improved Security: By reducing the number of passwords users need to manage, SSO decreases the attack surface and potential for password-related security breaches. It also allows for the implementation of stronger authentication methods.
? User Convenience: SSO improves the user experience by simplifying the login process, which can lead to higher productivity and satisfaction.
? References:

NEW QUESTION 5
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 6
A security analyst is reviewing the following log:

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

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

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

Answer: B

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

NEW QUESTION 7
A user submits a help desk ticket stating then account does not authenticate sometimes. An analyst reviews the following logs for the user:
Which of the following best explains the reason the user's access is being denied?

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

Answer: B

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

NEW QUESTION 8
During a security assessment using an CDR solution, a security engineer generates the following report about the assets in me system:

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

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

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

Answer: A

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

NEW QUESTION 9
Developers have been creating and managing cryptographic material on their personal laptops fix use in production environment. A security engineer needs to initiate a more secure process. Which of the following is the best strategy for the engineer to use?

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

Answer: D

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

NEW QUESTION 10
A security engineer is developing a solution to meet the following requirements?
• All endpoints should be able to establish telemetry with a SIEM.
• All endpoints should be able to be integrated into the XDR platform.
• SOC services should be able to monitor the XDR platform
Which of the following should the security engineer implement to meet the requirements?

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

Answer: D

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

NEW QUESTION 10
A security configure is building a solution to disable weak CBC configuration for remote access connections lo Linux systems. Which of the following should the security engineer modify?

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

Answer: D

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

NEW QUESTION 12
A company receives several complaints from customers regarding its website. An engineer implements a parser for the web server logs that generates the following output:

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

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

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

Answer: B

Explanation:
The table indicates varying load times for users accessing the website from different geographic locations. Customers from Australia and India are experiencing significantly higher load times compared to those from the United States. This suggests that latency and geographical distance are affecting the website's performance.
? A. IDS (Intrusion Detection System): While an IDS is useful for detecting malicious
activities, it does not address performance issues related to latency and geographical distribution of content.
? B. CDN (Content Delivery Network): A CDN stores copies of the website's content
in multiple geographic locations. By serving content from the nearest server to the user, a CDN can significantly reduce load times and improve user experience globally.
? C. WAF (Web Application Firewall): A WAF protects web applications by filtering and monitoring HTTP traffic but does not improve performance related to geographical latency.
? D. NAC (Network Access Control): NAC solutions control access to network
resources but are not designed to address web performance issues.

Implementing a CDN is the best solution to resolve the performance issues observed in the log output.
References:
? CompTIA Security+ Study Guide
? "CDN: Content Delivery Networks Explained" by Akamai Technologies
? NIST SP 800-44, "Guidelines on Securing Public Web Servers"

NEW QUESTION 16
A company's security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent IIS zero-day vulnerability was discovered that affects all versions of the Windows Server OS:

	OS	Externally available?	Behind WAF?	IIS installed?
Host 1	Windows 2019	Yes	Yes	Yes
Host 2	Windows 2008 R2	No	N/A	No
Host 3	Windows 2012 R2	Yes	Yes	Yes
Host 4	Windows 2022	Yes	No	Yes
Host 5	Windows 2012 R2	No	N/A	No
Host 6	Windows 2019	Yes	No	No

Which of the following hosts should a security analyst patch first once a patch is available?

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6

Answer: A

Explanation:
Based on the security policy that any publicly available server must be patched within 12 hours after a patch is released, the security analyst should patch Host 1 first. Here??s why:
? Public Availability: Host 1 is externally available, making it accessible from the
internet. Publicly available servers are at higher risk of being targeted by attackers, especially when a zero-day vulnerability is known.
? Exposure to Threats: Host 1 has IIS installed and is publicly accessible, increasing its exposure to potential exploitation. Patching this host first reduces the risk of a successful attack.
? Prioritization of Critical Assets: According to best practices, assets that are exposed to higher risks should be prioritized for patching to mitigate potential threats promptly.
? References:

NEW QUESTION 21
Which of the following AI concerns is most adequately addressed by input sanitation?

A. Model inversion
B. Prompt Injection
C. Data poisoning
D. Non-explainable model

Answer: B

Explanation:
Input sanitation is a critical process in cybersecurity that involves validating and cleaning data provided by users to prevent malicious inputs from causing harm. In the context of AI concerns:
? A. Model inversion involves an attacker inferring sensitive data from model
outputs, typically requiring sophisticated methods beyond just manipulating input data.
? B. Prompt Injection is a form of attack where an adversary provides malicious input
to manipulate the behavior of AI models, particularly those dealing with natural language processing (NLP). Input sanitation directly addresses this by ensuring that inputs are cleaned and validated to remove potentially harmful commands or instructions that could alter the AI's behavior.
? C. Data poisoning involves injecting malicious data into the training set to
compromise the model. While input sanitation can help by filtering out bad data, data poisoning is typically addressed through robust data validation and monitoring during the model training phase, rather than real-time input sanitation.
? D. Non-explainable model refers to the lack of transparency in how AI models
make decisions. This concern is not addressed by input sanitation, as it relates more to model design and interpretability techniques.
Input sanitation is most relevant and effective for preventing Prompt Injection attacks, where the integrity of user inputs directly impacts the performance and security of AI models.
References:
? CompTIA Security+ Study Guide
? "Security of Machine Learning" by Battista Biggio, Blaine Nelson, and Pavel Laskov
? OWASP (Open Web Application Security Project) guidelines on input validation and injection attacks
Top of Form Bottom of Form

NEW QUESTION 24
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 28
An organization wants to create a threat model to identity vulnerabilities in its infrastructure. Which of the following, should be prioritized first?

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

Answer: A

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

NEW QUESTION 29
A security analyst reviews the following report:

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

Which of the following assessments is the analyst performing?

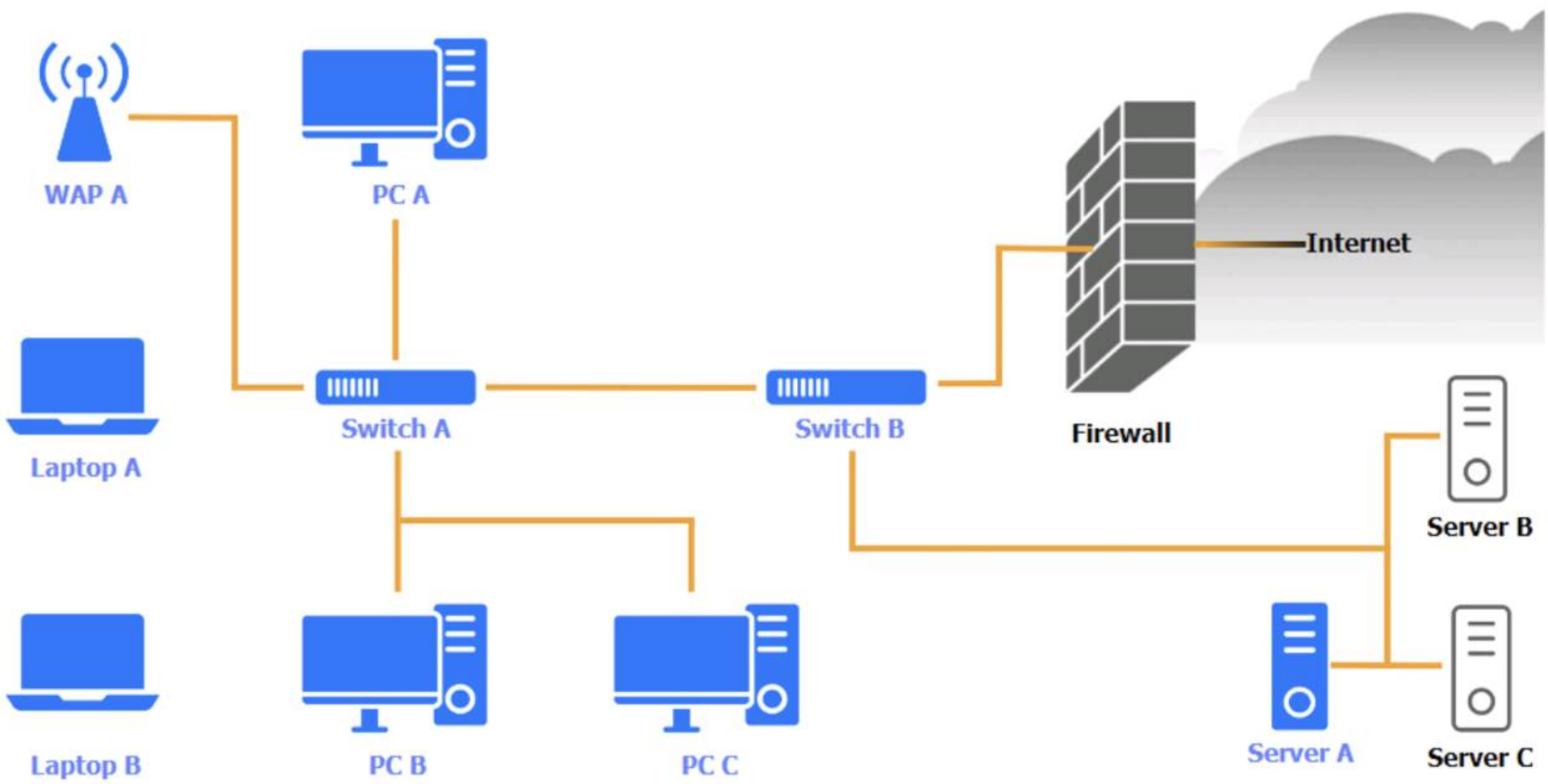
A. System
B. Supply chain
C. Quantitative
D. Organizational

Answer: B

Explanation:
The table shows detailed information about products, including location, chassis manufacturer, OS, application developer, and vendor. This type of information is typically assessed in a supply chain assessment to evaluate the security and reliability of components and services from different suppliers.
Why Supply Chain Assessment?
? Component Evaluation: Assessing the origin and security of each component used in the products, including hardware, software, and third-party services.
? Vendor Reliability: Evaluating the security practices and reliability of vendors involved in providing components or services.

? Risk Management: Identifying potential risks associated with the supply chain, such as vulnerabilities in third-party components or insecure development practices.
Other types of assessments do not align with the detailed supplier and component information provided:
? A. System: Focuses on individual system security, not the broader supply chain.
? C. Quantitative: Focuses on numerical risk assessments, not supplier information.
? D. Organizational: Focuses on internal organizational practices, not external
suppliers.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"
? "Supply Chain Security Best Practices," Gartner Research

NEW QUESTION 31
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

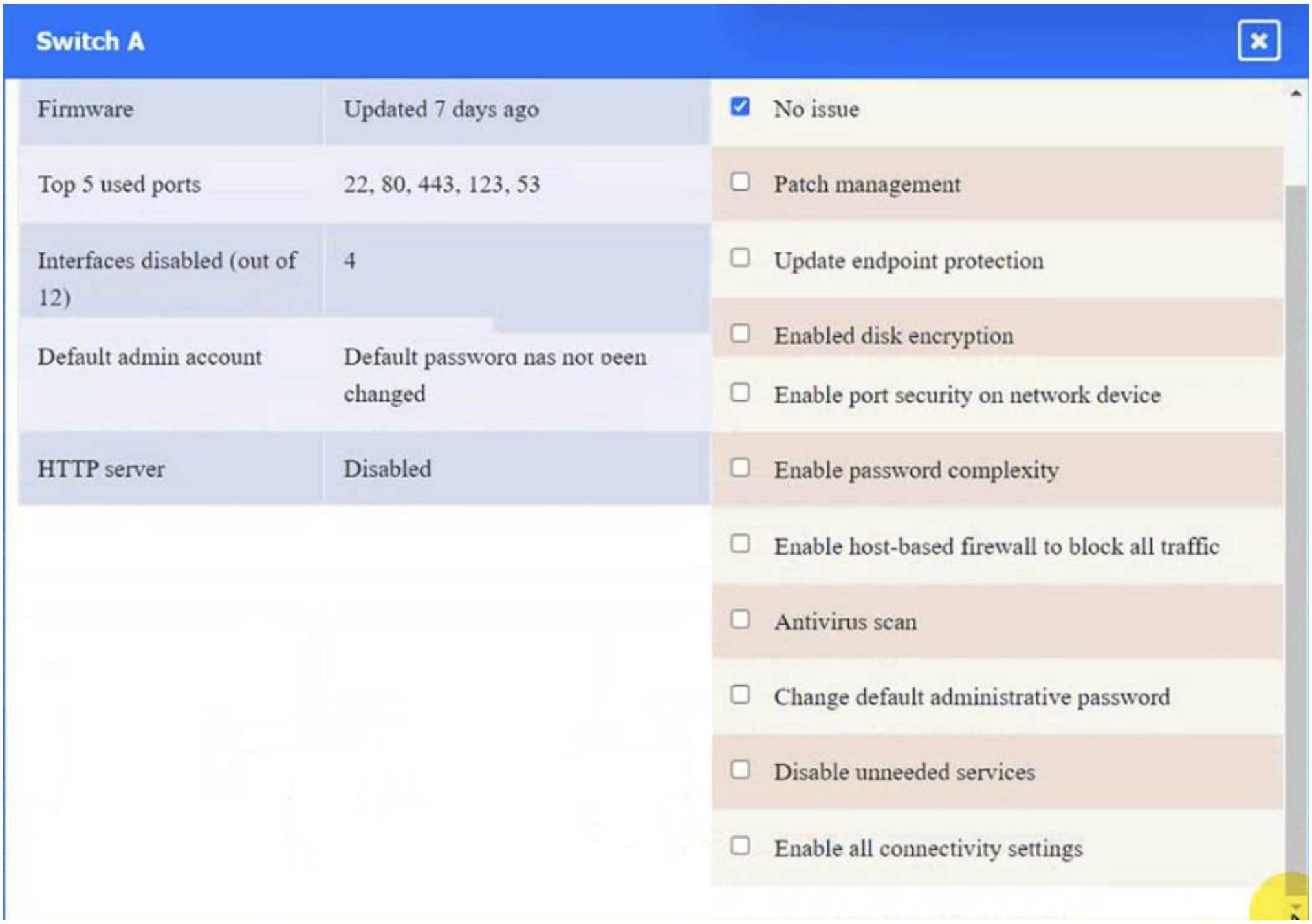
Laptop A

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

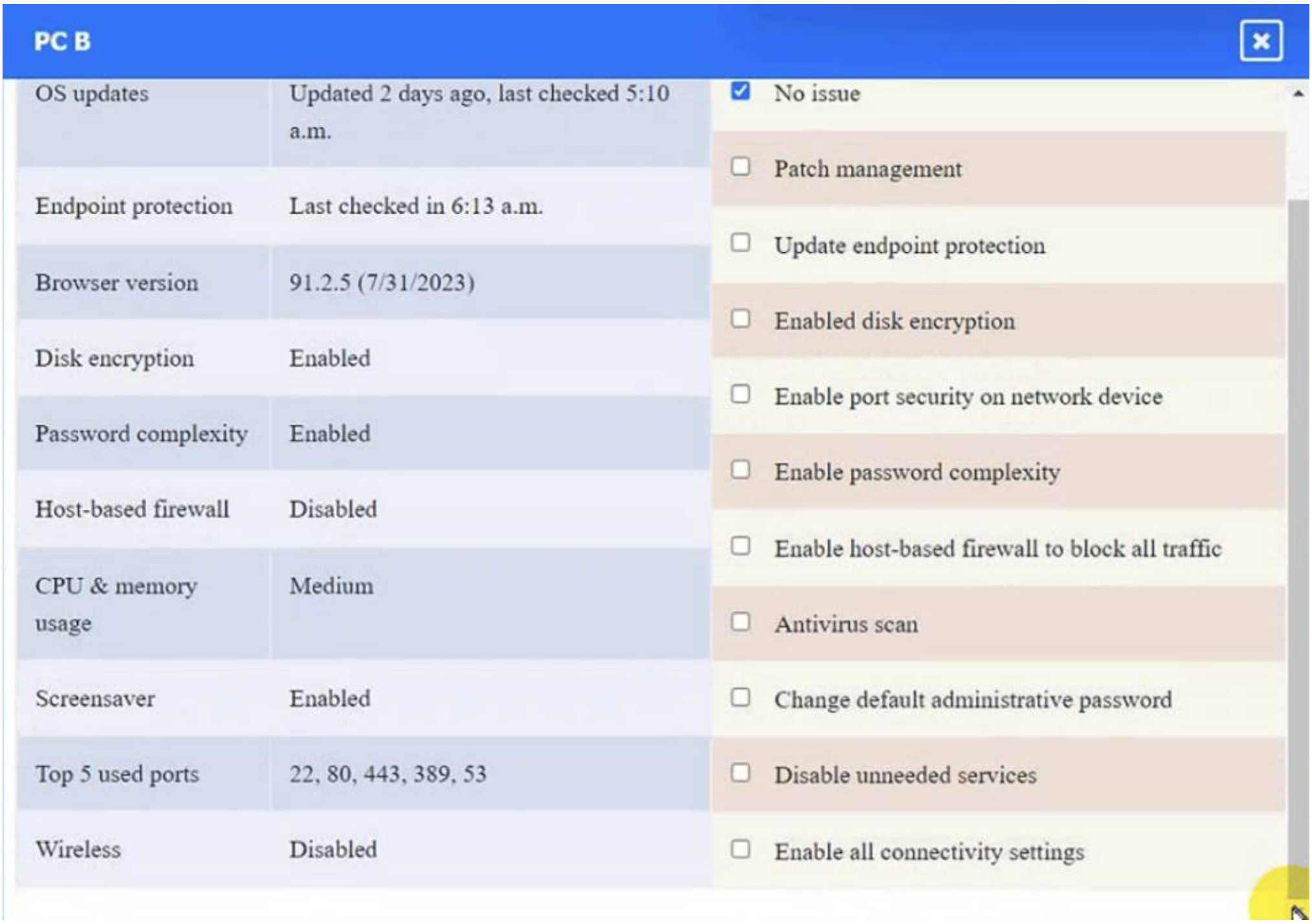
Firmware	Updated 7 days ago	☑ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
Interfaces disabled (out of 6)	1	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
		☐ Enable port security on network device
HTTP server	Disabled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

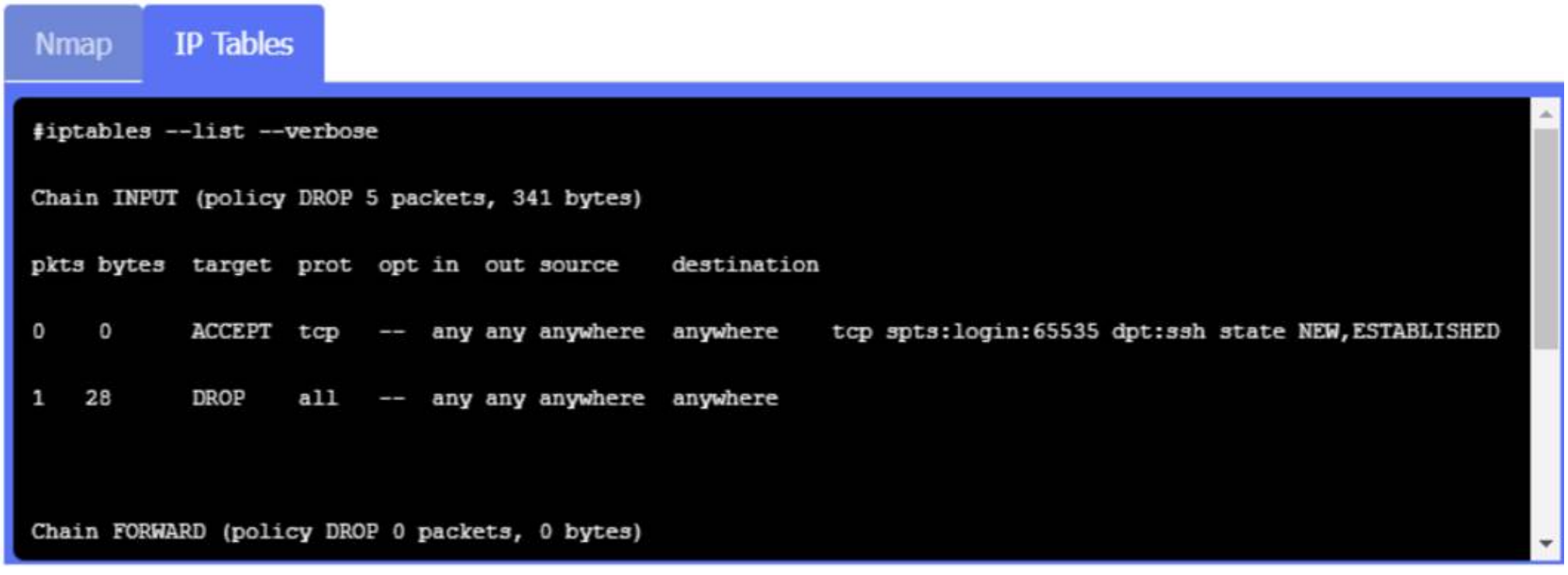
```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

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

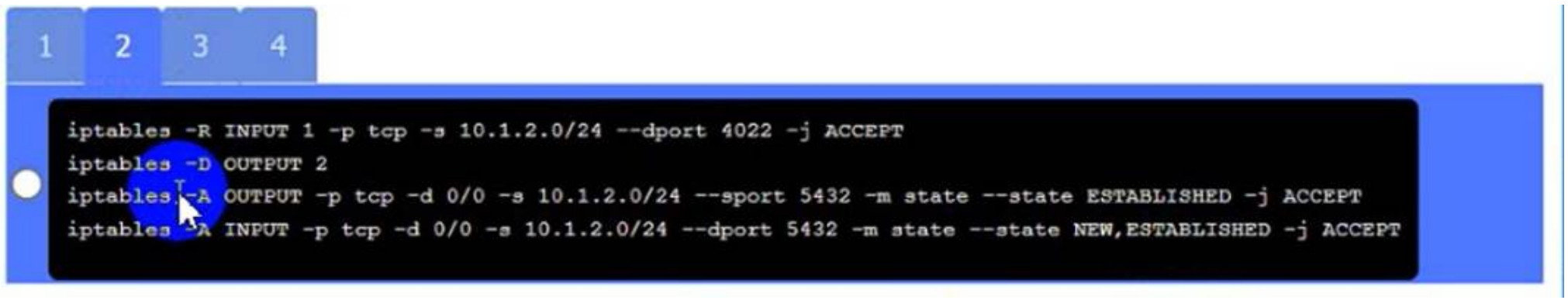
```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --dport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```



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 35
A company receives reports about misconfigurations and vulnerabilities in a third-party hardware device that is part of its released products. Which of the following solutions is the best way for the company to identify possible issues at an earlier stage?

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

Answer: D

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

NEW QUESTION 39
A financial technology firm works collaboratively with business partners in the industry to share threat intelligence within a central platform This collaboration gives partner organizations the ability to obtain and share data associated with emerging threats from a variety of adversaries Which of the following should the organization most likely leverage to facilitate this activity? (Select two).

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

Answer: DE

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

NEW QUESTION 44
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 46
A company wants to install a three-tier approach to separate the web. database, and application servers A security administrator must harden the environment which of the following is the best solution?

A. Deploying a VPN to prevent remote locations from accessing server VLANs
B. Configuring a SASb solution to restrict users to server communication
C. Implementing microsegmentation on the server VLANs
D. installing a firewall and making it the network core

Answer: C

Explanation:
The best solution to harden a three-tier environment (web, database, and application servers) is to implement microsegmentation on the server VLANs. Here??s why:
? Enhanced Security: Microsegmentation creates granular security zones within the
data center, allowing for more precise control over east-west traffic between servers. This helps prevent lateral movement by attackers who may gain access to one part of the network.
? Isolation of Tiers: By segmenting the web, database, and application servers, the
organization can apply specific security policies and controls to each segment, reducing the risk of cross-tier attacks.
? Compliance and Best Practices: Microsegmentation aligns with best practices for
network security and helps meet compliance requirements by ensuring that sensitive data and systems are properly isolated and protected.
? References:

NEW QUESTION 47
A vulnerability can on a web server identified the following:

```
* TLS 1.2 Cipher Suitea:
The aerver accepted the following 4 cipher auitea:
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 50
A systems administrator works with engineers to process and address vulnerabilities as a result of continuous scanning activities. The primary challenge faced by the administrator is differentiating between valid and invalid findings. Which of the following would the systems administrator most likely verify is properly configured?

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

Answer: B

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

References:
? CompTIA SecurityX Study Guide: Highlights the importance of using valid credentials for accurate vulnerability scanning.
? "Vulnerability Management" by Park Foreman: Discusses the role of scanning credentials in obtaining accurate scan results and minimizing false positives.
? "The Art of Network Security Monitoring" by Richard Bejtlich: Covers best practices for configuring and using vulnerability scanning tools, including the need for valid credentials.

NEW QUESTION 55
A security analyst needs to ensure email domains that send phishing attempts without previous communications are not delivered to mailboxes The following email headers are being reviewed

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

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

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

Answer: D

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

NEW QUESTION 60
After remote desktop capabilities were deployed in the environment, various vulnerabilities were noticed.
• Exfiltration of intellectual property
• Unencrypted files
• Weak user passwords
Which of the following is the best way to mitigate these vulnerabilities? (Select two).

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

Answer: AE

Explanation:
To mitigate the identified vulnerabilities, the following solutions are most appropriate:
? A. Implementing data loss prevention (DLP): DLP solutions help prevent the
unauthorized transfer of data outside the organization. This directly addresses the exfiltration of intellectual property by monitoring, detecting, and blocking sensitive data transfers.
? E. Enabling modern authentication that supports Multi-Factor Authentication
(MFA): This significantly enhances security by requiring additional verification methods beyond just passwords. It addresses the issue of weak user passwords by making it much harder for unauthorized users to gain access, even if they obtain the password.
Other options, while useful in specific contexts, do not address all the vulnerabilities mentioned:
? B. Deploying file integrity monitoring helps detect changes to files but does not
prevent data exfiltration or address weak passwords.
? C. Restricting access to critical file services improves security but is not comprehensive enough to mitigate all identified vulnerabilities.
? D. Deploying directory-based group policies can enforce security policies but might not directly prevent data exfiltration or ensure strong authentication.

? F. Implementing a version control system helps manage changes to files but is not a security measure for preventing the identified vulnerabilities.
? G. Implementing a CMDB platform (Configuration Management Database) helps manage IT assets but does not address the specific security issues mentioned.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"
? CIS Controls, "Control 13: Data Protection" and "Control 16: Account Monitoring and Control"

NEW QUESTION 63
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 67
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 68
The material finding from a recent compliance audit indicate a company has an issue with excessive permissions. The findings show that employees changing roles or departments results in privilege creep. Which of the following solutions are the best ways to mitigate this issue? (Select two).
Setting different access controls defined by business area

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

Answer: AD

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

NEW QUESTION 70
A security analyst wants to use lessons learned from a poor incident response to reduce dwell lime in the future The analyst is using the following data points

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

Which of the following would the analyst most likely recommend?

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

Answer: C

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

NEW QUESTION 71
A network engineer must ensure that always-on VPN access is enabled Curt restricted to company assets Which of the following best describes what the engineer needs to do"

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

Answer: A

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

References:
? CompTIA SecurityX Study Guide
? "Device Certificates for VPN Access," Cisco Documentation
? NIST Special Publication 800-77, "Guide to IPsec VPNs"

NEW QUESTION 75
A security engineer needs 10 secure the OT environment based on me following requirements
• Isolate the OT network segment
• Restrict Internet access.
• Apply security updates two workstations
• Provide remote access to third-party vendors
Which of the following design strategies should the engineer implement to best meet these requirements?

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

Answer: B

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

NEW QUESTION 77
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 80
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 81
While reviewing recent modem reports, a security officer discovers that several employees were contacted by the same individual who impersonated a recruiter. Which of the following best describes this type of correlation?

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

Answer: A

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

NEW QUESTION 82
SIMULATION
During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.
INSTRUCTIONS
Review each of the events and select the appropriate analysis and remediation options for each IoC.

IoC 1 | IoC 2 | IoC 3

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

Analysis: Select analysis

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

Remediation: Select remediation

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

IoC 1 | IoC 2 | IoC 3

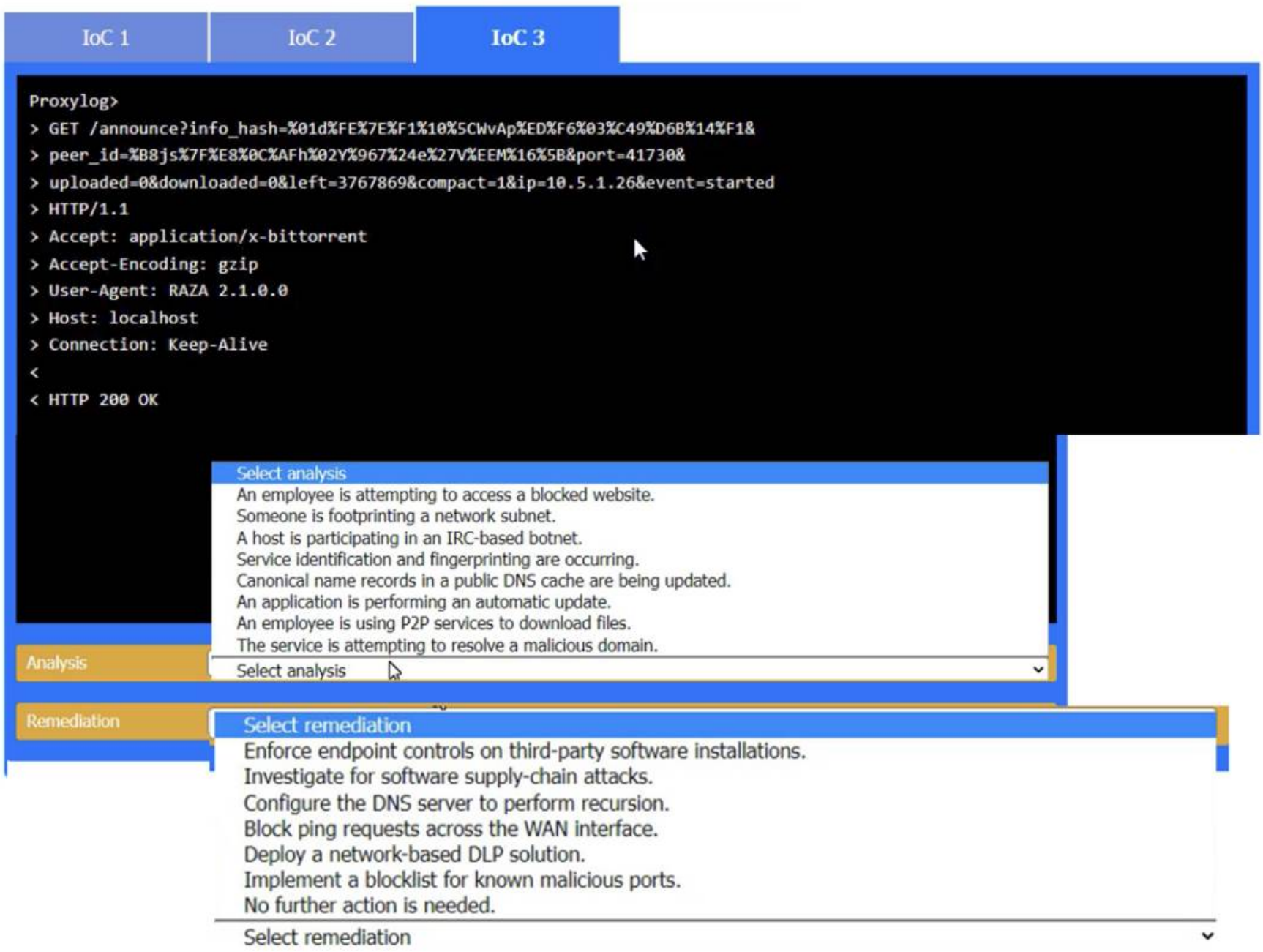
```
Src        Dst        Proto     Data   Action
10.0.5.5   10.1.2.1   IP_ICMP   ECHO   Drop
10.0.5.5   10.1.2.2   IP_ICMP   ECHO   Drop
10.0.5.5   10.1.2.3   IP_ICMP   ECHO   Drop
10.0.5.5   10.1.2.4   IP_ICMP   ECHO   Drop
10.0.5.5   10.1.2.5   IP_ICMP   ECHO   Drop
```

Analysis: Select analysis

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

Remediation: Select remediation

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



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Analysis and Remediation Options for Each IoC: IoC 1:
? Evidence:
? Analysis:
? Remediation:
IoC 2:
? Evidence:
? Analysis:
? Remediation:
IoC 3:
? Evidence:
? Analysis:
? Remediation:
References:
? CompTIA Security+ Study Guide: This guide offers detailed explanations on identifying and mitigating various types of Indicators of Compromise (IoCs) and the corresponding analysis and remediation strategies.
? CompTIA Security+ Exam Objectives: These objectives cover key concepts in network security monitoring and incident response, providing guidelines on how to handle different types of security events.
? Security Operations Center (SOC) Best Practices: This resource outlines effective strategies for analyzing and responding to anomalous events within a SOC, including the use of blocklists, endpoint controls, and network configuration
changes.
By accurately analyzing the nature of each IoC and applying the appropriate remediation measures, the organization can effectively mitigate potential security threats and maintain a robust security posture.

NEW QUESTION 83
After an incident response exercise, a security administrator reviews the following table:

Service	Risk rating	Criticality rating	Alert severity
Public website	Medium	Low	Low
Email	High	High	High
Human resources systems	High	Medium	Medium
Phone system	High	Critical	Critical
Intranet	Low	Low	Low

Which of the following should the administrator do to beat support rapid incident response in the future?

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

Answer: B

Explanation:
Enabling dashboards for service status monitoring is the best action to support rapid incident response. The table shows various services with different risk, criticality, and alert severity ratings. To ensure timely and effective incident response, real-time visibility into the status of these services is crucial.
Why Dashboards for Service Status Monitoring?
? Real-time Visibility: Dashboards provide an at-a-glance view of the current status of all critical services, enabling rapid detection of issues.
? Centralized Monitoring: A single platform to monitor the status of multiple services helps streamline incident response efforts.
? Proactive Alerting: Dashboards can be configured to show alerts and anomalies immediately, ensuring that incidents are addressed as soon as they arise.
? Improved Decision Making: Real-time data helps incident response teams make informed decisions quickly, reducing downtime and mitigating impact.
Other options, while useful, do not offer the same level of comprehensive, real-time visibility and proactive alerting:
? A. Automate alerting to IT support for phone system outages: This addresses one
service but does not provide a holistic view.
? C. Send emails for failed log-in attempts on the public website: This is a specific alert for one type of issue and does not cover all services.
? D. Configure automated isolation of human resources systems: This is a reactive measure for a specific service and does not provide real-time status monitoring.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"
? "Best Practices for Implementing Dashboards," Gartner Research

NEW QUESTION 86
A security review revealed that not all of the client proxy traffic is being captured. Which of the following architectural changes best enables the capture of traffic for analysis?

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

Answer: C

Explanation:
Configuring a span port on the perimeter firewall to ingest logs is the best architectural change to ensure that all client proxy traffic is captured for analysis.
Here??s why:
? Comprehensive Traffic Capture: A span port (or mirror port) on the perimeter
firewall can capture all inbound and outbound traffic, including traffic that might bypass the proxy. This ensures that all network traffic is available for analysis.
? Centralized Logging: By capturing logs at the perimeter firewall, the organization
can centralize logging and analysis, making it easier to detect and investigate anomalies.
? Minimal Disruption: Implementing a span port is a non-intrusive method that does
not require significant changes to the network architecture, thus minimizing disruption to existing services.
? References:

NEW QUESTION 91
.....

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