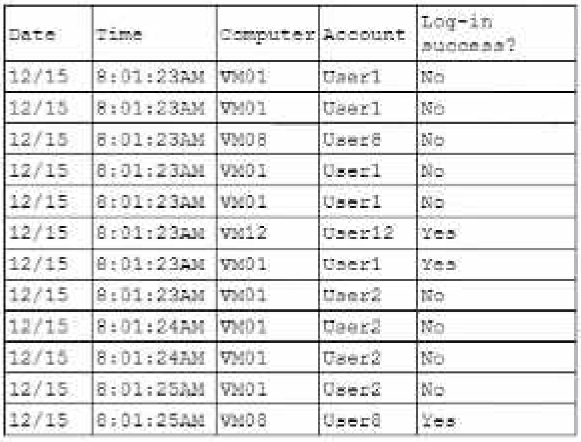
Product Questions: 134
Version: 5.1

Question: 1

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:
VM01 at 8:01:23 AM
VM08 at 8:01:23 AM
VM01 at 8:01:23 AM
VM08 at 8:01:23 AM
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.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
CompTIA Security+ Certification Exam Objectives
NIST Special Publication 800-63B: Digital Identity Guidelines
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.

Question: 2

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.
Reference:
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

Question: 3

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.
Reference:
CompTIA Security+ SY0-601 Official Study Guide by Quentin Docter, Jon Buhagiar
NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations

Question: 4

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.

Question: 5

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

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

Answer: B

Explanation:

Building playbooks for different scenarios and performing regular table-top exercises directly addresses the issues identified in the lessons-learned review. Here's why:
Lost important information for further analysis: Playbooks outline step-by-step procedures for incident response, ensuring that team members know exactly what to document and how to preserve evidence.
Did not utilize the chain of communication: Playbooks include communication protocols, specifying who to notify and when. Regular table-top exercises reinforce these communication channels, ensuring they are followed during actual incidents.
Did not follow the right steps for a proper response: Playbooks provide a clear sequence of actions to be taken during various types of incidents, helping the team to respond in a structured and effective manner. Regular exercises allow the team to practice these steps, identifying and correcting any deviations from the plan.
Investing in better forensic tools (Option A) or requiring certifications (Option C) are also valuable,

but they do not directly address the procedural and communication gaps identified. Publishing and enforcing the incident response policy (Option D) is important but not as practical and hands-on as playbooks and exercises in ensuring the team is prepared.
Reference:
CompTIA Security+ Study Guide
NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"
SANS Institute, "Incident Handler's Handbook"

Question: 6

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: A, E

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.
Reference:

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"

Question: 7

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

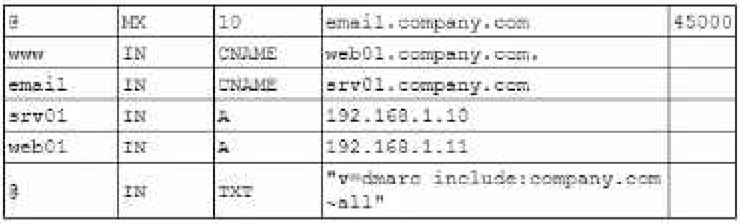
Answer: A

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.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NSA's Guide to the Secure Configuration of Red Hat Enterprise Linux 5 (SELinux)
NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations

Question: 8

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: D, B

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.
DMARC: Ensuring the DMARC record is correctly set up helps in preventing email spoofing and phishing, aligning with email security best practices.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
RFC 7489: Domain-based Message Authentication, Reporting & Conformance (DMARC)
NIST Special Publication 800-45: Guidelines on Electronic Mail Security

Question: 9

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.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
ISA/IEC 62443 Standards: Security for Industrial Automation and Control Systems

Question: 10

All organization is concerned about insider threats from employees who have individual access to encrypted material. Which of the following techniques best addresses this issue?

A. SSO with MFA
B. Sating and hashing
C. Account federation with hardware tokens
D. SAE
E. Key splitting

Answer: E

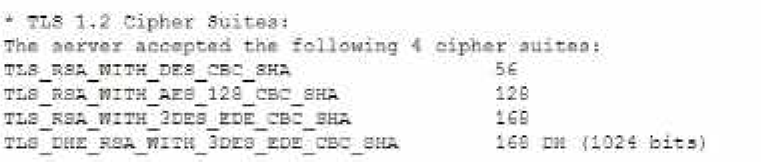
Explanation:

The technique that best addresses the issue of insider threats from employees who have individual access to encrypted material is key splitting. Here’s why:
Key Splitting: Key splitting involves dividing a cryptographic key into multiple parts and distributing these parts among different individuals or systems. This ensures that no single individual has complete access to the key, thereby mitigating the risk of insider threats.
Increased Security: By requiring multiple parties to combine their key parts to access encrypted material, key splitting provides an additional layer of security. This approach is particularly useful in environments where sensitive data needs to be protected from unauthorized access by insiders.
Compliance and Best Practices: Key splitting aligns with best practices and regulatory requirements for handling sensitive information, ensuring that access is tightly controlled and monitored.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-57: Recommendation for Key Management

ISO/IEC 27002:2013: Information Technology - Security Techniques - Code of Practice for Information Security Controls
By employing key splitting, organizations can effectively reduce the risk of insider threats and enhance the overall security of encrypted material.

Question: 11

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: B, C

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.
Reference:
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

Question: 12

The identity and access management team is sending logs to the SIEM for continuous monitoring.

The deployed log collector is forwarding logs to
the SIEM. However, only false positive alerts are being generated. Which of the following is the most likely reason for the inaccurate alerts?

A. The compute resources are insufficient to support the SIEM
B. The SIEM indexes are 100 large
C. The data is not being properly parsed
D. The retention policy is not property configured

Answer: C

Explanation:

Proper parsing of data is crucial for the SIEM to accurately interpret and analyze the logs being forwarded by the log collector. If the data is not parsed correctly, the SIEM may misinterpret the logs, leading to false positives and inaccurate alerts. Ensuring that the log data is correctly parsed allows the SIEM to correlate and analyze the logs effectively, which is essential for accurate alerting and monitoring.

Question: 13

An incident response team is analyzing malware and observes the following:
• Does not execute in a sandbox
• No network loCs
• No publicly known hash match
• No process injection method detected
Which of the following should the team do next to proceed with further analysis?

A. Use an online vims analysis tool to analyze the sample
B. Check for an anti-virtualization code in the sample
C. Utilize a new deployed machine to run the sample.
D. Search oilier internal sources for a new sample.

Answer: B

Explanation:

Malware that does not execute in a sandbox environment often contains anti-analysis techniques, such as anti-virtualization code. This code detects when the malware is running in a virtualized environment and alters its behavior to avoid detection. Checking for anti-virtualization code is a logical next step because:
It helps determine if the malware is designed to evade analysis tools.
Identifying such code can provide insights into the malware's behavior and intent.
This step can also inform further analysis methods, such as running the malware on physical hardware.
Reference:
CompTIA Security+ Study Guide

SANS Institute, "Malware Analysis Techniques"
"Practical Malware Analysis" by Michael Sikorski and Andrew Honig

Question: 14

Which of the following best explains the importance of determining organization risk appetite when operating with a constrained budget?

A. Risk appetite directly impacts acceptance of high-impact low-likelihood events.
B. Organizational risk appetite varies from organization to organization
C. Budgetary pressure drives risk mitigation planning in all companies
D. Risk appetite directly influences which breaches are disclosed publicly

Answer: A

Explanation:

Risk appetite is the amount of risk an organization is willing to accept to achieve its objectives. When operating with a constrained budget, understanding the organization's risk appetite is crucial because:
It helps prioritize security investments based on the level of risk the organization is willing to tolerate.
High-impact, low-likelihood events may be deemed acceptable if they fall within the organization's risk appetite, allowing for budget allocation to other critical areas.
Properly understanding and defining risk appetite ensures that limited resources are used effectively to manage risks that align with the organization's strategic goals.
Reference:
CompTIA Security+ Study Guide
NIST Risk Management Framework (RMF) guidelines
ISO 31000, "Risk Management – Guidelines"

Question: 15

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.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-57: Recommendation for Key Management
ISO/IEC 19790:2012: Information Technology - Security Techniques - Security Requirements for Cryptographic Modules

Question: 16

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.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management
OWASP Authentication Cheat Sheet

Question: 17

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: A, D

Explanation:

To mitigate the issue of excessive permissions and privilege creep, the best solutions are:
Implementing a Role-Based Access Policy:
Role-Based Access Control (RBAC): This policy ensures that access permissions are granted based on the user's role within the organization, aligning with the principle of least privilege. Users are only granted access necessary for their role, reducing the risk of excessive permissions.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations
Performing Periodic Access Reviews:
Regular Audits: Periodic access reviews help identify and rectify instances of privilege creep by ensuring that users' access permissions are appropriate for their current roles. These reviews can highlight unnecessary or outdated permissions, allowing for timely adjustments.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
ISO/IEC 27001:2013 - Information Security Management

Question: 18

A security architect is establishing requirements to design resilience in un enterprise system trial will be extended to other physical locations. The system must

- Be survivable to one environmental catastrophe
- Re recoverable within 24 hours of critical loss of availability
- Be resilient to active exploitation of one site-to-site VPN solution

A. Load-balance connection attempts and data Ingress at internet gateways
B. Allocate fully redundant and geographically distributed standby sites.
C. Employ layering of routers from diverse vendors
D. Lease space to establish cold sites throughout other countries
E. Use orchestration to procure, provision, and transfer application workloads lo cloud services
F. Implement full weekly backups to be stored off-site for each of the company's sites

Answer: B

Explanation:

To design resilience in an enterprise system that can survive environmental catastrophes, recover within 24 hours, and be resilient to active exploitation, the best strategy is to allocate fully redundant and geographically distributed standby sites. Here's why:

Geographical Redundancy: Having geographically distributed standby sites ensures that if one site is affected by an environmental catastrophe, the other sites can take over, providing continuity of operations.

Full Redundancy: Fully redundant sites mean that all critical systems and data are replicated, enabling quick recovery in the event of a critical loss of availability.

Resilience to Exploitation: Distributing resources across multiple sites reduces the risk of a single point of failure and increases resilience against targeted attacks.

Reference:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

NIST Special Publication 800-34: Contingency Planning Guide for Federal Information Systems

ISO/IEC 27031:2011 - Guidelines for Information and Communication Technology Readiness for Business Continuity

Question: 19

Users must accept the terms presented in a captive petal when connecting to a guest network. Recently, users have reported that they are unable to access the Internet after joining the network A network engineer observes the following:

• Users should be redirected to the captive portal.

• The Motive portal runs Tl. S 1 2

• Newer browser versions encounter security errors that cannot be bypassed

• Certain websites cause unexpected re directs

Which of the following mow likely explains this behavior?

A. The TLS ciphers supported by the captive portal ate deprecated

B. Employment of the HSTS setting is proliferating rapidly.

C. Allowed traffic rules are causing the NIPS to drop legitimate traffic

D. An attacker is redirecting supplicants to an evil twin WLAN.

Answer: A

Explanation:

The most likely explanation for the issues encountered with the captive portal is that the TLS ciphers supported by the captive portal are deprecated. Here's why:

TLS Cipher Suites: Modern browsers are continuously updated to support the latest security standards and often drop support for deprecated and insecure cipher suites. If the captive portal uses outdated TLS ciphers, newer browsers may refuse to connect, causing security errors.

HSTS and Browser Security: Browsers with HTTP Strict Transport Security (HSTS) enabled will not allow connections to sites with weak security configurations. Deprecated TLS ciphers would cause these browsers to block the connection.

Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-52: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
OWASP Transport Layer Protection Cheat Sheet
By updating the TLS ciphers to modern, supported ones, the security engineer can ensure compatibility with newer browser versions and resolve the connectivity issues reported by users.

Question: 20

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

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

Answer: D

Explanation:

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

Question: 21

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.
Reference:
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"

Question: 22

A software development team requires valid data for internal tests. Company regulations, however do not allow the use of this data in cleartext. Which of the following solutions best meet these requirements?

A. Configuring data hashing
B. Deploying tokenization
C. Replacing data with null record
D. Implementing data obfuscation

Answer: B

Explanation:

Tokenization replaces sensitive data elements with non-sensitive equivalents, called tokens, that can be used within the internal tests. The original data is stored securely and can be retrieved if necessary. This approach allows the software development team to work with data that appears realistic and valid without exposing the actual sensitive information.
Configuring data hashing (Option A) is not suitable for test data as it transforms the data into a fixed-length value that is not usable in the same way as the original data. Replacing data with null records (Option C) is not useful as it does not provide valid data for testing. Data obfuscation (Option D) could be an alternative but might not meet the regulatory requirements as effectively as tokenization.
Reference:
CompTIA Security+ Study Guide
NIST SP 800-57 Part 1 Rev. 5, "Recommendation for Key Management"
PCI DSS Tokenization Guidelines

Question: 23

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

A. Limn the platform's abilities to only non-sensitive functions
B. Enhance the training model's effectiveness.
C. Grant the system the ability to self-govern
D. Require end-user acknowledgement of organizational policies.

Answer: A

Explanation:
Limiting the platform's abilities to only non-sensitive functions helps to mitigate risks associated with AI operations. By ensuring that the AI-enabled digital worker is only allowed to perform tasks that do not involve sensitive or critical data, the organization reduces the potential impact of any security breaches or misuse.
Enhancing the training model's effectiveness (Option B) is important but does not directly address security guardrails. Granting the system the ability to self-govern (Option C) could increase risk as it may act beyond the organization's control. Requiring end-user acknowledgement of organizational policies (Option D) is a good practice but does not implement technical guardrails to secure the AI environment.
Reference:
CompTIA Security+ Study Guide
NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"
ISO/IEC 27001, "Information Security Management"

Question: 24

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.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-88: Guidelines for Media Sanitization
ISO/IEC 27002:2013 - Information Security Management

Question: 25

A company hosts a platform-as-a-service solution with a web-based front end, through which customer interact with data sets. A security administrator needs to deploy controls to prevent application-focused attacks. Which of the following most directly supports the administrator's objective'

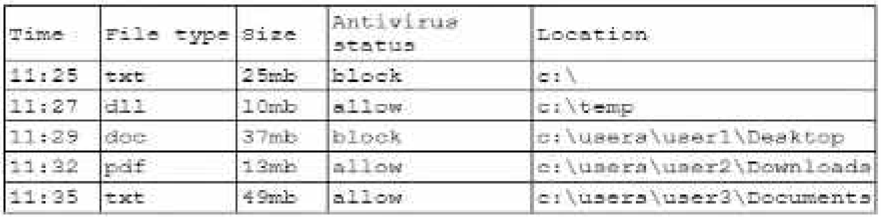
A. improving security dashboard visualization on SIEM
B. Rotating API access and authorization keys every two months
C. Implementing application toad balancing and cross-region availability
D. Creating WAF policies for relevant programming languages

Answer: D

Explanation:
The best way to prevent application-focused attacks for a platform-as-a-service solution with a web-based front end is to create Web Application Firewall (WAF) policies for relevant programming languages. Here's why:
Application-Focused Attack Prevention: WAFs are designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. They help prevent attacks such as SQL injection, cross-site scripting (XSS), and other application-layer attacks.
Customizable Rules: WAF policies can be tailored to the specific programming languages and frameworks used by the web application, providing targeted protection based on known vulnerabilities and attack patterns.
Real-Time Protection: WAFs provide real-time protection, blocking malicious requests before they reach the application, thereby enhancing the security posture of the platform.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
OWASP Top Ten: Web Application Security Risks
NIST Special Publication 800-95: Guide to Secure Web Services

Question: 26

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

Question: 27

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.