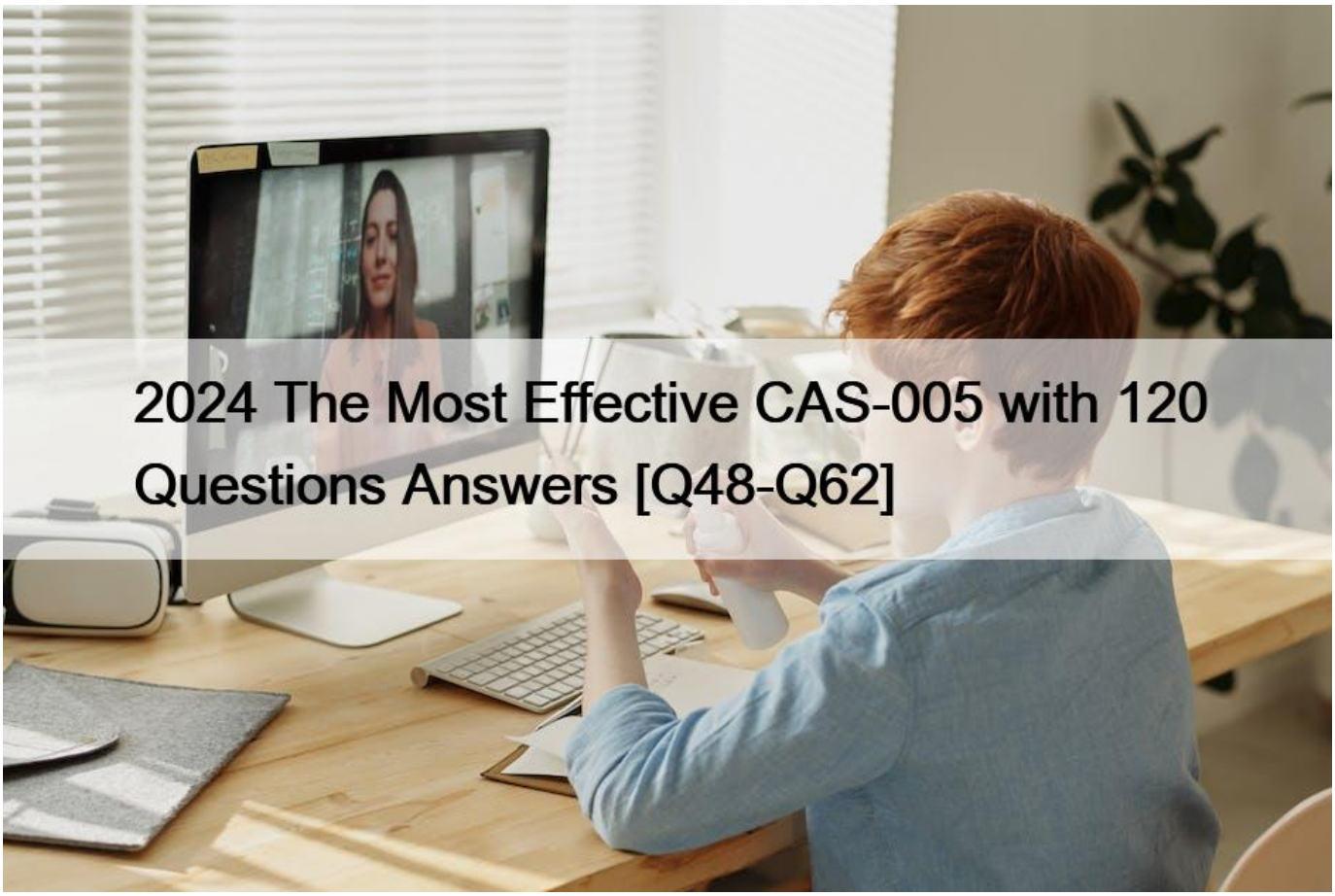
2024 The Most Effective CAS-005 with 120 Questions Answers [Q48-Q62



2024 The Most Effective CAS-005 with 120 Questions Answers Try Free and Start Using Realistic Verified CAS-005 Dumps Instantly. Q48. 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?
* Sigma rules
* Ariel Query Language
* UBA rules and use cases
* TAXII/STIX library

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.

Q49. A central bank implements strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin. Which of the following best describes the cyberthreat to the bank?
* Ability to obtain components during wartime
* Fragility and other availability attacks
* Physical Implants and tampering
* Non-conformance to accepted manufacturing standards
The best description of the cyber threat to a central bank implementing strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin, is the risk of physical implants and tampering. Here’s why:

* Supply Chain Security: The supply chain is a critical vector for hardware tampering and physical implants, which can compromise the integrity and security of hardware components before they reach the organization.

* Targeted Attacks: Banks and financial institutions are high-value targets, making them susceptible to sophisticated attacks, including those involving physical implants that can be introduced during manufacturing or shipping processes.

* Strict Mitigations: Implementing an allow list for specific countries aims to mitigate the risk of supply chain attacks by limiting the sources of hardware. However, the primary concern remains the introduction of malicious components through tampering.

* References:

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

* NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations

* ISO/IEC 20243:2018 – Information Technology – Open Trusted Technology Provider Standard

Q50. A company is having issues with its vulnerability management program New devices/lPs are added and dropped regularly, making the vulnerability report inconsistent Which of the following actions should the company lake to most likely improve the vulnerability management process’
* Request a weekly report with all new assets deployed and decommissioned
* Extend the DHCP lease lime to allow the devices to remain with the same address for a longer period.
* Implement a shadow IT detection process to avoid rogue devices on the network
* Perform regular discovery scanning throughout the 11 landscape using the vulnerability management tool
To improve the vulnerability management process in an environment where new devices/IPs are added and dropped regularly, the company should perform regular discovery scanning throughout the IT landscape using the vulnerability management tool. Here’s why:

* Accurate Asset Inventory: Regular discovery scans help maintain an up-to-date inventory of all assets, ensuring that the vulnerability management process includes all relevant devices and IPs.

* Consistency in Reporting: By continuously discovering and scanning new and existing assets, the company can generate consistent

and comprehensive vulnerability reports that reflect the current state of the network.

* Proactive Management: Regular scans enable the organization to proactively identify and address vulnerabilities on new and existing assets, reducing the window of exposure to potential threats.

* References:

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

* NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies

* CIS Controls: Control 1 – Inventory and Control of Hardware Assets

Q51. 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?
* Automate alerting to IT support for phone system outages.
* Enable dashboards for service status monitoring
* Send emails for failed log-In attempts on the public website
* Configure automated Isolation of human resources systems

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

Q52. 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’
* improving security dashboard visualization on SIEM
* Rotating API access and authorization keys every two months
* Implementing application toad balancing and cross-region availability
* Creating WAF policies for relevant programming languages
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.

* References:

* 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

Q53. A software engineer is creating a CI/CD pipeline to support the development of a web application The DevSecOps team is required to identify syntax errors Which of the following is the most relevant to the DevSecOps team’s task’
* Static application security testing
* Software composition analysis
* Runtime application self-protection
* Web application vulnerability scanning
Static Application Security Testing (SAST) involves analyzing source code or compiled code for security vulnerabilities without executing the program. This method is well-suited for identifying syntax errors, coding standards violations, and potential security

issues early in the development lifecycle.

* A. Static application security testing (SAST): SAST tools analyze the source code to detect syntax errors, vulnerabilities, and other issues before the code is run. This is the most relevant task for the DevSecOps team to identify syntax errors and improve code quality.

* B. Software composition analysis: This focuses on identifying vulnerabilities in open-source components and libraries used in the application but does not address syntax errors directly.

* C. Runtime application self-protection (RASP): RASP involves monitoring and protecting applications during runtime, which does not help in identifying syntax errors during the development phase.

* D. Web application vulnerability scanning: This involves scanning the running application for vulnerabilities but does not address syntax errors in the code.

References:

* CompTIA Security+ Study Guide

* OWASP (Open Web Application Security Project) guidelines on SAST

* NIST SP 800-95, “Guide to Secure Web Services”

Top of Form

Bottom of Form

Q54. 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?
* Disable User2’s account
* Disable User12’s account
* Disable User8’s account
* Disable User1’s account

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.

* References:

* 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.

Q55. 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?
* Increasing password complexity to require 31 least 16 characters
* implementing an SSO solution and integrating with applications
* Requiring users to use an open-source password manager
* Implementing an MFA solution to avoid reliance only on passwords
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:

* 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

Q56. After some employees were caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation. Which of the following would the company most likely do to decrease this type of risk?
* Improve firewall rules to avoid access to those platforms.
* Implement a cloud-access security broker
* Create SIEM rules to raise alerts for access to those platforms
* Deploy an internet proxy that filters certain domains

A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Implementing a CASB provides several benefits:

* A. Improve firewall rules to avoid access to those platforms: This can help but is not as effective or comprehensive as a CASB.

* B. Implement a cloud-access security broker: A CASB can provide visibility into cloud application usage, enforce data security policies, and protect against data leaks by monitoring and controlling access to cloud services. It also provides advanced features like data encryption, data loss prevention (DLP), and compliance monitoring.

* C. Create SIEM rules to raise alerts for access to those platforms: This helps in monitoring but does not prevent data leaks.

* D. Deploy an internet proxy that filters certain domains: This can block access to specific sites but lacks the granular control and visibility provided by a CASB.

Implementing a CASB is the most comprehensive solution to decrease the risk of data leaks by providing visibility, control, and enforcement of security policies for cloud services.

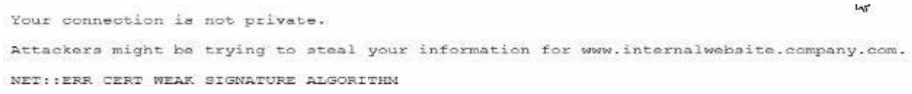
References:

* CompTIA Security+ Study Guide

* Gartner, “Magic Quadrant for Cloud Access Security Brokers”

* NIST SP 800-144, “Guidelines on Security and Privacy in Public Cloud Computing”

Q57. A security analyst received a report that an internal web page is down after a company-wide update to the web browser Given the following error message:



Which of the following is the best way to fix this issue?
* Rewriting any legacy web functions
* Disabling all deprecated ciphers
* Blocking all non-essential pons

* Discontinuing the use of self-signed certificates
The error message “NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM” indicates that the web browser is rejecting the certificate because it uses a weak signature algorithm. This commonly happens with self-signed certificates, which often use outdated or insecure algorithms.

Why Discontinue Self-Signed Certificates?

* Security Compliance: Modern browsers enforce strict security standards and may reject certificates that do not comply with these standards.

* Trusted Certificates: Using certificates from a trusted Certificate Authority (CA) ensures compliance with security standards and is less likely to be flagged as insecure.

* Weak Signature Algorithm: Self-signed certificates might use weak algorithms like MD5 or SHA-1, which are considered insecure.

Other options do not address the specific cause of the certificate error:

* A. Rewriting legacy web functions: Does not address the certificate issue.

* B. Disabling deprecated ciphers: Useful for improving security but not related to the certificate error.

* C. Blocking non-essential ports: This is unrelated to the issue of certificate validation.

References:

* CompTIA SecurityX Study Guide

* “Managing SSL/TLS Certificates,” OWASP

* “Best Practices for Certificate Management,” NIST Special Publication 800-57

Q58. 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?
* The TLS ciphers supported by the captive portal ate deprecated
* Employment of the HSTS setting is proliferating rapidly.
* Allowed traffic rules are causing the NIPS to drop legitimate traffic
* An attacker is redirecting supplicants to an evil twin WLAN.
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.

* References:

* 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.

Q59. 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).
* CWPP
* YAKA
* ATTACK
* STIX
* TAXII
* JTAG
* 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”

Q60. A company’s security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent llS 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?
* 1
* 2
* 3
* 4
* 5
* 6

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:

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

* NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies

* CIS Controls: Control 3 – Continuous Vulnerability Management

Q61. 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	9.7s	207
Microsoft Edge	Australia	6.4s	200

which of the following should the company implement to best resolve the issue?
* IDS
* CDN
* WAF
* NAC
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”

Q62. 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?
* Requesting budget for better forensic tools to Improve technical capabilities for Incident response operations
* Building playbooks for different scenarios and performing regular table-top exercises

* Requiring professional incident response certifications tor each new team member
* Publishing the incident response policy and enforcing it as part of the security awareness program

Building playbooks for different scenarios and performing regular table-top exercises directly addresses the issues identified in the lessons-learned review. Here’s why:

* Lost important information for further analysis: Playbooks outline step-by-step procedures for incident response, ensuring that team members know exactly what to document and how to preserve evidence.

* Did not utilize the chain of communication: Playbooks include communication protocols, specifying who to notify and when. Regular table-top exercises reinforce these communication channels, ensuring they are followed during actual incidents.

* Did not follow the right steps for a proper response: Playbooks provide a clear sequence of actions to be taken during various types of incidents, helping the team to respond in a structured and effective manner. Regular exercises allow the team to practice these steps, identifying and correcting any deviations from the plan.

Investing in better forensic tools (Option A) or requiring certifications (Option C) are also valuable, but they do not directly address the procedural and communication gaps identified. Publishing and enforcing the incident response policy (Option D) is important but not as practical and hands-on as playbooks and exercises in ensuring the team is prepared.

References:

* CompTIA Security+ Study Guide

* NIST SP 800-61 Rev. 2, “Computer Security Incident Handling Guide”

* SANS Institute, “Incident Handler’s Handbook”