Free Questions for CS0-003

Shared by Slater on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A security team conducts a lessons-learned meeting after struggling to determine who should conduct the next steps following a security event. Which of the following should the team create to address this issue?

Options:

A- Service-level agreement
B- Change management plan
C- Incident response plan
D- Memorandum of understanding

Answer:

C

Explanation:

An incident response plan (IRP) is a document that defines the roles and responsibilities, procedures, and guidelines for responding to a security incident. It helps the security team to act quickly and effectively, minimizing the impact and cost of the incident. An IRP should specify who should conduct the next steps following a security event, such as containment, eradication, recovery, and analysis12. Reference: CompTIA CySA+ CS0-003 Certification Study Guide, page 362; 6 Incident Response Steps to Take After a Security Event, section 2.

Question 2

Question Type: MultipleChoice

During a tabletop exercise, engineers discovered that an ICS could not be updated due to hardware versioning incompatibility. Which of the following is the most likely cause of this issue?

Options:

A- Legacy system
B- Business process interruption

C- Degrading functionality
D- Configuration management

Answer:

A

Explanation:

The most likely cause of the issue where an ICS (Industrial Control System) could not be updated due to hardware versioning incompatibility is a legacy system. Legacy systems often have outdated hardware and software that may not be compatible with modern updates and patches. This can pose significant challenges in maintaining security and operational efficiency.

Question 3

Question Type: MultipleChoice

Several reports with sensitive information are being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

Options:

A- Implement step-up authentication for administrators.
B- Improve employee training and awareness.
C- Increase password complexity standards.
D- Deploy mobile device management.

Answer:

B

Explanation:

Improving employee training and awareness is the best option to address the issue of sensitive reports being disclosed via file sharing services. By educating employees about the risks of unapproved file sharing, the security protocols to follow, and the proper channels to use for sharing company information, an organization can significantly reduce the risk of sensitive data being accidentally or intentionally shared on insecure platforms. This human-centric approach

addresses the root cause of the problem. Options A, C, and D are security controls that do not directly address the behavior of sharing sensitive files on unauthorized services.

Question 4

Question Type: MultipleChoice

A cybersecurity analyst has been assigned to the threat-hunting team to create a dynamic detection strategy based on behavioral analysis and attack patterns. Which of the following best describes what the analyst will be creating?

Options:

A- Bots
B- IoCs
C- TTPs
D- Signatures

Answer:

C

Explanation:

The analyst will be creating TTPs (Tactics, Techniques, and Procedures). TTPs describe the behavior, methods, and patterns used by attackers during a cyber attack. By focusing on TTPs, the analyst can develop a dynamic detection strategy that identifies malicious activities based on the observed behavior and patterns, rather than relying on static indicators like signatures or IOCs (Indicators of Compromise).

Question 5

Question Type: MultipleChoice

A security analyst is trying to validate the results of a web application scan with Burp Suite. The security analyst performs the following:

Which of the following vulnerabilitles Is the securlty analyst trylng to valldate?

Options:

A- SQL injection
B- LFI
C- XSS
D- CSRF

Answer:

B

Explanation:

The security analyst is validating a Local File Inclusion (LFI) vulnerability, as indicated by the ''/.../.../.../'' in the GET request which is a common indicator of directory traversal attempts associated with LFI. The other options are not relevant for this purpose: SQL injection involves injecting malicious SQL statements into a database query; XSS involves injecting malicious scripts into a web page; CSRF involves tricking a user into performing an unwanted action on a web application.

According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to ''use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities''. The book also covers the usage and syntax of Burp Suite, a tool used for testing web application security, in chapter 6. Specifically, it explains the meaning and function of each component in Burp Suite, such as Repeater, which allows the security analyst to modify and resend individual requests1, page 239. Therefore, this is a reliable source to verify

the answer to the question.

Question 6

Question Type: MultipleChoice

An organization's email account was compromised by a bad actor. Given the following Information:

Time	Description
8:30 a.m.	A total of 2,000 emails were sent from the compromised account. The email directed the recipients to pay an invoice. Enclosed in the email was a short message, along with a link and an attachment was contained in the email.
8:45 a.m.	Recipients started alerting the organization's help desk about the email.
8:55 a.m.	The help desk escalated the issue to the CSIRT.
9:10 a.m.	The IRT was assembled, a call bridge was established, and the Chief Information Security Officer declared an incident.
9:15 a.m.	The web session for the email account was revoked and password resets were initiated. The machine was investigated further to ensure security controls were in place.
9:30 a.m.	All sent emails were removed from organization's servers.
9:35 a.m.	The CSIRT lowered the priority of the incident and started to review logs.
9:45 a.m.	Passwords were reset for all internal users that clicked on the link.
9:50 a.m.	Continued analysis to determine the impact was limited.
10:30 a.m.	Besides continued monitoring, the organization reasonably believed the threat was remediated.

Which of the following is the length of time the team took to detect the threat?

Options:

A- 25 minutes
B- 40 minutes
C- 45 minutes
D- 2 hours

Answer:

B

Explanation:

The threat was detected from the time the emails were sent at 8:30 a.m. to when the recipients started alerting the organization's help desk about the email at 8:45 a.m., taking a total of 15 minutes. The detection time is the time elapsed between the occurrence of an incident and its discovery by the security team . The other options are either too short or too long based on the given information. Reference: : Detection Time : Incident Response Metrics: Mean Time to Detect and Mean Time to Respond

Question 7

Question Type: MultipleChoice

A list of loCs released by a government security organization contains the SHA-256 hash for a Microsoft-signed legitimate binary, svchost. exe. Which of the following best describes the result if security teams add this indicator to their detection signatures?

Options:

A- This indicator would fire on the majority of Windows devices.
B- Malicious files with a matching hash would be detected.
C- Security teams would detect rogue svchost. exe processes in their environment.
D- Security teams would detect event entries detailing execution of known-malicious svchost. exe processes.

Answer:

A

Explanation:

Adding the SHA-256 hash of a legitimate Microsoft-signed binary like svchost.exe to detection signatures would result in the indicator firing on the majority of Windows devices. Svchost.exe is a common and legitimate system process used by Windows, and using its hash as an indicator of compromise (IOC) would generate numerous false positives, as it would match the legitimate

instances of svchost.exe running on all Windows systems.

Question 8

Question Type: MultipleChoice

A network analyst notices a long spike in traffic on port 1433 between two IP addresses on opposite sides of a WAN connection. Which of the following is the most likely cause?

Options:

A- A local red team member is enumerating the local RFC1918 segment to enumerate hosts.
B- A threat actor has a foothold on the network and is sending out control beacons.
C- An administrator executed a new database replication process without notifying the SOC.
D- An insider threat actor is running Responder on the local segment, creating traffic replication.

Answer:

C

Explanation:

Port 1433 is commonly used by Microsoft SQL Server, which is a database management system. A spike in traffic on this port between two IP addresses on opposite sides of a WAN connection could indicate a database replication process, which is a way of copying and distributing data from one database server to another. This could be a legitimate activity performed by an administrator, but it should be communicated to the security operations center (SOC) to avoid confusion and false alarms.

Question 9

Question Type: MultipleChoice

A security team identified several rogue Wi-Fi access points during the most recent network scan. The network scans occur once per quarter. Which of the following controls would best all ow the organization to identity rogue devices more quickly?

Options:

A- Implement a continuous monitoring policy.
B- Implement a BYOD policy.
C- Implement a portable wireless scanning policy.
D- Change the frequency of network scans to once per month.

Answer:

A

Explanation:

The best control to allow the organization to identify rogue devices more quickly is

A) Implement a continuous monitoring policy. A continuous monitoring policy is a set of procedures and tools that enable an organization to detect and respond to unauthorized or anomalous activities on its network in real time or near real time. A continuous monitoring policy can help identify rogue access points as soon as they appear on the network, rather than waiting for quarterly or monthly scans.A continuous monitoring policy can also help improve the overall security posture and compliance of the organization by providing timely and accurate information about its network assets, vulnerabilities, threats, and incidents1.

Question 10

Question Type: MultipleChoice

The Chief Executive Officer (CEO) has notified that a confidential trade secret has been compromised. Which of the following communication plans should the CEO initiate?

Options:

A- Alert department managers to speak privately with affected staff.
B- Schedule a press release to inform other service provider customers of the compromise.
C- Disclose to all affected parties in the Chief Operating Officer for discussion and resolution.
D- Verify legal notification requirements of PII and SPII in the legal and human resource departments.

Answer:

A

Explanation:

The CEO should initiate an alert to department managers to speak privately with affected staff. This is because the trade secret is confidential and should not be disclosed to the public. Additionally, the CEO should verify legal notification requirements of PII and SPII in the legal and human resource departments to ensure compliance with data protection laws.

Question 11

Question Type: MultipleChoice

A security analyst is reviewing the logs of a web server and notices that an attacker has attempted to exploit a SQL injection vulnerability. Which of the following tools can the analyst use to analyze the attack and prevent future attacks?

Options:

A- A web application firewall
B- A network intrusion detection system
C- A vulnerability scanner
D- A web proxy

Answer:

A

Explanation:

A web application firewall (WAF) is a tool that can protect web servers from attacks such as SQL injection, cross-site scripting, and other web-based threats. A WAF can filter, monitor, and block malicious HTTP traffic before it reaches the web server. A WAF can also be configured with rules and policies to detect and prevent specific types of attacks.

: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

Question 12

Question Type: MultipleChoice

Which of the following explains the importance of a timeline when providing an incident response report?

Options:

A- The timeline contains a real-time record of an incident and provides information that helps to simplify a postmortem analysis.
B- An incident timeline provides the necessary information to understand the actions taken to mitigate the threat or risk.
C- The timeline provides all the information, in the form of a timetable, of the whole incident response process including actions taken.
D- An incident timeline presents the list of commands executed by an attacker when the system was compromised, in the form of a timetable.

Answer:

C

Explanation:

An incident response timeline is a detailed chronological record of all events and actions taken during the response to a security incident. It includes timestamps and descriptions of each step, providing a comprehensive overview of how the incident was detected, contained, mitigated, and resolved. This timeline is crucial for post-incident analysis, helping to understand the effectiveness of the response, identify areas for improvement, and ensure accountability and transparency in the incident handling process.