CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

QUESTION 1

A Chief Information Security Officer (CISO) wants to disable a functionality on a business- critical web application that is vulnerable to RCE in order to maintain the minimum risk level with minimal increased cost. Which of the following risk treatments best describes what the CISO is looking for?

A. Transfer

B. Mitigate

C. Accept

D. Avoid

Correct Answer: B

Risk avoidance involves taking actions to eliminate the risk entirely, which in this case means disabling the vulnerable functionality to prevent the risk of Remote Code Execution (RCE). This approach ensures that the risk is not present, aligning with the CISO\\'s objective of maintaining minimal risk.

QUESTION 2

Which of the following describes the best reason for conducting a root cause analysis?

A. The root cause analysis ensures that proper timelines were documented.

B. The root cause analysis allows the incident to be properly documented for reporting.

C. The root cause analysis develops recommendations to improve the process.

D. The root cause analysis identifies the contributing items that facilitated the event.

Correct Answer: D

The root cause analysis identifies the contributing items that facilitated the event is the best reason for conducting a root cause analysis, as it reflects the main goal and benefit of this problem-solving approach. A root cause analysis (RCA) is a process of discovering the root causes of problems in order to identify appropriate solutions. A root cause is the core issue or factor that sets in motion the entire cause-and-effect chain that leads to the problem. A root cause analysis assumes that it is more effective to systematically prevent and solve underlying issues rather than just treating symptoms or putting out fires. A root cause analysis can be performed using various methods, tools, and techniques that help to uncover the causes of problems, such as events and causal factor analysis, change analysis, barrier analysis, or fishbone diagrams. A root cause analysis can help to improve quality, performance, safety, or efficiency by finding and eliminating the sources of problems. The other options are not as accurate as the root cause analysis identifies the contributing items that facilitated the event, as they do not capture the essence or value of conducting a root cause analysis. The root cause analysis ensures that proper timelines were documented is a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting timelines can help to establish the sequence of events and actions that led to the problem, but it does not necessarily identify or address the root causes. The root cause analysis allows the incident to be properly documented for reporting is also a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting and reporting incidents can help to communicate and share information about problems and solutions, but it does not necessarily identify or address the root causes. The root cause analysis develops recommendations to improve the process is another possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Developing recommendations can help to implement solutions and prevent future problems, but it does not necessarily identify or address the root causes.

QUESTION 3

An analyst needs to forensically examine a Windows machine that was compromised by a threat actor. Intelligence reports state this specific threat actor is characterized by hiding malicious artifacts, especially with alternate data streams. Based on this intelligence, which of the following BEST explains alternate data streams?

A. A different way data can be streamlined if the user wants to use less memory on a Windows system for forking resources.

B. A way to store data on an external drive attached to a Windows machine that is not readily accessible to users.

C. A Windows attribute that provides for forking resources and is potentially used to hide the presence of secret or malicious files inside the file records of a benign file.

D. A Windows attribute that can be used by attackers to hide malicious files within system memory.

Correct Answer: C

QUESTION 4

A security administrator has been notified by the IT operations department that some vulnerability reports contain an incomplete list of findings. Which of the following methods should be used to resolve this issue?

A. Credentialed scar

B. External scan

C. Differential scan

D. Network scan

Correct Answer: A

A credentialed scan is a type of vulnerability scan that uses valid credentials to log in to the scanned systems and perform a more thorough and accurate assessment of their vulnerabilities. A credentialed scan can access more information than a non-credentialed scan, such as registry keys, patch levels, configuration settings, and installed applications. A credentialed scan can also reduce the number of false positives and false negatives, as it can verify the actual state of the system rather than relying on inference or assumptions. The other types of scans are not related to the issue of incomplete findings, as they refer to different aspects of vulnerability scanning, such as the scope, location, or frequency of the scan. An external scan is a scan that is performed from outside the network perimeter, usually from the internet. An external scan can reveal how an attacker would see the network and what vulnerabilities are exposed to the public. An external scan cannot access internal systems or resources that are behind firewalls or other security controls. A differential scan is a scan that compares the results of two scans and highlights the differences between them. A differential scan can help identify changes in the network environment, such as new vulnerabilities, patched vulnerabilities, or new devices. A differential scan does not provide a complete list of findings by itself, but rather a summary of changes. A network scan is a scan that focuses on the network layer of the OSI model and detects vulnerabilities related to network devices, protocols, services, and configurations. A network scan can discover open ports, misconfigured firewalls, unencrypted traffic, and other network-related issues. A network scan does not provide information about the application layer or the host layer of the OSI model, such as web applications or operating systems.

Reference: https://www.splunk.com/en_us/blog/learn/vulnerability-scanning.html

QUESTION 5

Which of the following techniques would be best to provide the necessary assurance for embedded software that drives centrifugal pumps at a power Plant?

A. Containerization

B. Manual code reviews

C. Static and dynamic analysis

D. Formal methods

Correct Answer: D

According to the CompTIA CySA+ Study Guide: S0-003, 3rd Edition1, the best technique to provide the necessary assurance for embedded software that drives centrifugal pumps at a power plant is formal methods. Formal methods are a rigorous and mathematical approach to software development and verification, which can ensure the correctness and reliability of critical software systems. Formal methods can be used to specify, design, implement, and verify embedded software using formal languages, logics, and tools1. Containerization, manual code reviews, and static and dynamic analysis are also useful techniques for software assurance, but they are not as rigorous or comprehensive as formal methods. Containerization is a method of isolating and packaging software applications with their dependencies, which can improve security, portability, and scalability. Manual code reviews are a process of examining the source code of a software program by human reviewers, which can help identify errors, vulnerabilities, and compliance issues. Static and dynamic analysis are techniques of testing and evaluating software without executing it (static) or while executing it (dynamic), which can help detect bugs, defects, and performance issues1.

QUESTION 6

A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

A. SLA

B. MOU

C. NDA

D. Limitation of liability

Correct Answer: A

SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

QUESTION 7

Due to an incident involving company devices, an incident responder needs to take a mobile phone to the lab for further investigation. Which of the following tools should be used to maintain the integrity of the mobile phone while it is transported? (Select two).

A. Signal-shielded bag

B. Tamper-evident seal

C. Thumb drive

D. Crime scene tape

E. Write blocker

F. Drive duplicator

Correct Answer: AB

A signal-shielded bag and a tamper-evident seal are tools that can be used to maintain the integrity of the mobile phone while it is transported. A signal-shielded bag prevents the phone from receiving or sending any signals that could compromise the data or evidence on the device. A tamper-evident seal ensures that the phone has not been opened or altered during the transportation. References: Mobile device forensics, Section: Acquisition

QUESTION 8

AXSS vulnerability was reported on one of the non-sensitive/non-mission-critical public websites of a company. The security department confirmed the finding and needs to provide a recommendation to the application owner. Which of the following recommendations will best prevent this vulnerability from being exploited? (Select two).

A. Implement an IPS in front of the web server.

B. Enable MFA on the website.

C. Take the website offline until it is patched.

D. Implement a compensating control in the source code.

E. Configure TLS v1.3 on the website.

F. Fix the vulnerability using a virtual patch at the WAF.

Correct Answer: DF

The best recommendations to prevent an XSS vulnerability from being exploited are to implement a compensating control in the source code and to fix the vulnerability using a virtual patch at the WAF. A compensating control is a technique

that mitigates the risk of a vulnerability by adding additional security measures, such as input validation, output encoding, or HTML sanitization. A virtual patch is a rule that blocks or modifies malicious requests or responses at the WAF level,

without modifying the application code. These recommendations are effective, efficient, and less disruptive than the other options. References: CompTIA CySA+ Study Guide: S0-003, 3rd Edition, Chapter 4:

Security Operations and Monitoring, page 156; Cross Site Scripting Prevention Cheat Sheet, Section: XSS Defense Philosophy.

QUESTION 9

Which of the following would a security analyst most likely use to compare TTPs between different known adversaries of an organization?

A. MITRE ATTACK

B. Cyber Kill Cham

C. OWASP

D. STIXTAXII

Correct Answer: A

MITRE ATTandCK is a framework and knowledge base that describes the tactics, techniques, and procedures (TTPs) used by various adversaries in cyberattacks. MITRE ATTandCK can help security analysts compare TTPs between different known adversaries of an organization, as well as identify patterns, gaps, or trends in adversary behavior. MITRE ATTandCK can also help security analysts improve threat detection, analysis, and response capabilities, as well as share threat intelligence with other organizations or communities

QUESTION 10

A company is implementing a vulnerability management program and moving from an on-premises environment to a hybrid IaaS cloud environment. Which of the following implications should be considered on the new hybrid environment?

A. The current scanners should be migrated to the cloud

B. Cloud-specific misconfigurations may not be detected by the current scanners

C. Existing vulnerability scanners cannot scan laaS systems

D. Vulnerability scans on cloud environments should be performed from the cloud

Correct Answer: B

Cloud-specific misconfigurations are security issues that arise from improper or inadequate configuration of cloud resources, such as storage buckets, databases, virtual machines, or containers. Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the "re, one of the implications that should be considered on the new hybrid environment is that cloud-specific misconfigurations may not be detected by the current scanners.

QUESTION 11

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?

A. Legacy system

B. Business process interruption

C. Degrading functionality

D. Configuration management

Correct Answer: A

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 12

Which of the following would help to minimize human engagement and aid in process improvement in security operations?

A. OSSTMM

B. SIEM

C. SOAR

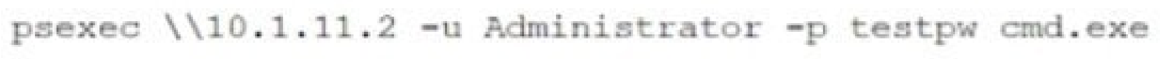
D. QVVASP

Correct Answer: C

SOAR stands for security orchestration, automation, and response, which is a term that describes a set of tools, technologies, or platforms that can help streamline, standardize, and automate security operations and incident response processes and tasks. SOAR can help minimize human engagement and aid in process improvement in security operations by reducing manual work, human errors, response time, or complexity. SOAR can also help enhance collaboration, coordination, efficiency, or effectiveness of security operations and incident response teams.

QUESTION 13

While reviewing system logs, a network administrator discovers the following entry:



```
psexec \\10.1.11.2 -u Administrator -p testpw cmd.exe
```

Which of the following occurred?

A. An attempt was made to access a remote workstation.

B. The PsExec services failed to execute.

C. A remote shell failed to open.

D. A user was trying to download a password file from a remote system.

Correct Answer: A

QUESTION 14

An organization is concerned about the security posture of vendors with access to its facilities and systems. The organization wants to implement a vendor review process to ensure the policies implemented by vendors are in line with its own. Which of the following will provide the highest assurance of compliance?

A. An in-house red-team report

B. A vendor self-assessment report

C. An independent third-party audit report

D. Internal and external scans from an approved third-party vulnerability vendor

Correct Answer: C

QUESTION 15

An older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. Which of the following factors would an analyst most likely communicate as the reason for this escalation?

A. Scope

B. Weaponization

C. CVSS

D. Asset value

Correct Answer: B

Weaponization is a factor that describes how an adversary develops or acquires an exploit or payload that can take advantage of a vulnerability and deliver a malicious effect. Weaponization can increase the severity or impact of a vulnerability, as it makes it easier or more likely for an attacker to exploit it successfully and cause damage or harm. Weaponization can also indicate the level of sophistication or motivation of an attacker, as well as the availability or popularity of an exploit or payload in the cyber threat landscape. In this case, an older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. This indicates that weaponization was the reason for this escalation.