CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following is a reason to take a DevSecOps approach to a software assurance program?

A. To find and fix security vulnerabilities earlier in the development process

B. To speed up user acceptance testing in order to deliver the code to production faster

C. To separate continuous integration from continuous development in the SDLC

D. To increase the number of security-related bug fixes worked on by developers

Correct Answer: A

QUESTION 2

A security analyst needs to secure digital evidence related to an incident. The security analyst must ensure that the accuracy of the data cannot be repudiated. Which of the following should be implemented?

A. Offline storage

B. Evidence collection

C. Integrity validation

D. Legal hold

Correct Answer: C

Integrity validation is the process of ensuring that the digital evidence has not been altered or tampered with during collection, acquisition, preservation, or analysis. It usually involves generating and verifying cryptographic hashes of the evidence, such as MD5 or SHA-1. Integrity validation is essential for maintaining the accuracy and admissibility of the digital evidence in court.

QUESTION 3

Which of the following describes the difference between intentional and unintentional insider threats\\'?

A. Their access levels will be different

B. The risk factor will be the same

C. Their behavior will be different

D. The rate of occurrence will be the same

Correct Answer: C

The difference between intentional and unintentional insider threats is their behavior. Intentional insider threats are malicious actors who deliberately misuse their access to harm the organization or its assets. Unintentional insider threats are

careless or negligent users who accidentally compromise the security of the organization or its assets. Their access levels, risk factors, and rates of occurrence may vary depending on various factors, but their behavior is the main distinction.

Reference:

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 12;

https://www.cisa.gov/sites/default/files/publications/Insider_Threat_Mitigation_Guide_508.pdf

QUESTION 4

A security analyst has identified a new malware file that has impacted the organization. The malware is polymorphic and has built-in conditional triggers that require a connection to the internet. The CPU has an idle process of at least 70%. Which of the following best describes how the security analyst can effectively review the malware without compromising the organization\\'s network?

A. Utilize an RDP session on an unused workstation to evaluate the malware.

B. Disconnect and utilize an existing infected asset off the network.

C. Create a virtual host for testing on the security analyst workstation.

D. Subscribe to an online service to create a sandbox environment.

Correct Answer: D

A sandbox environment is a safe and isolated way to analyze malware without affecting the organization\\'s network. An online service can provide a sandbox environment without requiring the security analyst to set up a virtual host or use an RDP session. Disconnecting and using an existing infected asset is risky and may not provide accurate results. References: Malware Analysis: Steps and Examples, Dynamic Analysis

QUESTION 5

Two employees in the finance department installed a freeware application that contained embedded malware. The network is robustly segmented based on areas of responsibility. These computers had critical sensitive information stored locally that needs to be recovered. The department manager advised all department employees to turn off their computers until the security team could be contacted about the issue. Which of the following is the first step the incident response staff members should take when they arrive?

A. Turn on all systems, scan for infection, and back up data to a USB storage device.

B. Identify and remove the software installed on the impacted systems in the department.

C. Explain that malware cannot truly be removed and then reimage the devices.

D. Log on to the impacted systems with an administrator account that has privileges to perform backups.

E. Segment the entire department from the network and review each computer offline.

Correct Answer: E

Segmenting the entire department from the network and reviewing each computer offline is the first step the incident

response staff members should take when they arrive. This step can help contain the malware infection and prevent it from spreading to other systems or networks. Reviewing each computer offline can help identify the source and scope of the infection, and determine the best course of action for recovery12. Turning on all systems, scanning for infection, and backing up data to a USB storage device is a risky step, as it can activate the malware and cause further damage or data loss. It can also compromise the USB storage device and any other system that connects to it. Identifying and removing the software installed on the impacted systems in the department is a possible step, but it should be done after segmenting the department from the network and reviewing each computer offline. Explaining that malware cannot truly be removed and then reimaging the devices is a drastic step, as it can result in data loss and downtime. It should be done only as a last resort, and after backing up the data and verifying its integrity. Logging on to the impacted systems with an administrator account that has privileges to perform backups is a dangerous step, as it can expose the administrator credentials and privileges to the malware, and allow it to escalate its access and capabilities34.
References: Incident Response: Processes, Best Practices and Tools - Atlassian, Incident Response Best Practices | SANS Institute, Malware Removal: How to Remove Malware from Your Device, How to Remove Malware From Your PC | PCMag

CS0-003 PDF Dumps CS0-003 VCE Dumps CS0-003 Study Guide