



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.pass4itsure.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**

An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?

- A. Eradication
- B. Recovery
- C. Containment
- D. Preparation

Correct Answer: A

Eradication is a step in the incident response process that involves removing any traces or remnants of the incident from the affected systems or networks, such as malware, backdoors, compromised accounts, or malicious files. Eradication also involves restoring the systems or networks to their normal or secure state, as well as verifying that the incident is completely eliminated and cannot recur. In this case, the analyst is remediating items associated with a recent incident by isolating the vulnerability and actively removing it from the system. This describes the eradication step of the incident response process.

QUESTION 2

During a company's most recent incident, a vulnerability in custom software was exploited on an externally facing server by an APT. The lessons-learned report noted the following:

The development team used a new software language that was not supported by the security team's automated assessment tools.

During the deployment, the security assessment team was unfamiliar with the new language and struggled to evaluate the software during advanced testing. Therefore, the vulnerability was not detected. The current IPS did not have effective

signatures and policies in place to detect and prevent runtime attacks on the new application.

To allow this new technology to be deployed securely going forward, which of the following will BEST address these findings? (Choose two.)

- A. Train the security assessment team to evaluate the new language and verify that best practices for secure coding have been followed
- B. Work with the automated assessment-tool vendor to add support for the new language so these vulnerabilities are discovered automatically
- C. Contact the human resources department to hire new security team members who are already familiar with the new language
- D. Run the software on isolated systems so when they are compromised, the attacker cannot pivot to adjacent systems
- E. Instruct only the development team to document the remediation steps for this vulnerability
- F. Outsource development and hosting of the applications in the new language to a third-party vendor so the risk is



transferred to that provider

Correct Answer: AB

QUESTION 3

A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network. Which of the following would be missing from a scan performed with this configuration?

- A. Operating system version
- B. Registry key values
- C. Open ports
- D. IP address

Correct Answer: B

QUESTION 4

An incident response team is working with law enforcement to investigate an active web server compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must connect to a database server. Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Choose two).

- A. Drop the tables on the database server to prevent data exfiltration.
- B. Deploy EDR on the web server and the database server to reduce the adversary's capabilities.
- C. Stop the httpd service on the web server so that the adversary can not use web exploits.
- D. Use microsegmentation to restrict connectivity to/from the web and database servers.
- E. Comment out the HTTP account in the /etc/passwdfile of the web server.
- F. Move the database from the database server to the web server.

Correct Answer: BD

QUESTION 5

A security analyst is reviewing the findings of the latest vulnerability report for a company's web application. The web application accepts files for a Bash script to be processed if the files match a given hash. The analyst is able to submit files to the system due to a hash collision. Which of the following should the analyst suggest to mitigate the vulnerability



with the fewest changes to the current script and infrastructure?

- A. Deploy a WAF to the front of the application.
- B. Replace the current MD5 with SHA-256.
- C. Deploy an antivirus application on the hosting system.
- D. Replace the MD5 with digital signatures.

Correct Answer: B

This option involves changing the hash algorithm from the vulnerable MD5 to the more secure SHA-256. It addresses the hash collision vulnerability directly and doesn't require major changes to the existing infrastructure or script logic.

[CS0-003 PDF Dumps](#)

[CS0-003 Study Guide](#)

[CS0-003 Exam Questions](#)