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

A company\\'s security team is updating a section of the reporting policy that pertains to inappropriate use of resources (e.g., an employee who installs cryptominers on workstations in the office). Besides the security team, which of the following groups should the issue be escalated to first in order to comply with industry best practices?

A. Help desk

B. Law enforcement

C. Legal department

D. Board member

Correct Answer: C

When updating a reporting policy that pertains to inappropriate use of resources, it\\'s important to involve the legal department as one of the first steps. Inappropriate use of resources can have legal implications, and involving the legal department ensures that the policy aligns with legal regulations and requirements. They can provide guidance on the appropriate actions to take and help ensure that the policy is comprehensive and legally sound.

QUESTION 2

A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URIs that should be denied access prior to more in-depth scanning. Which of following best fits the type of scanning activity requested?

A. Uncredentialed scan

B. Discovery scan

C. Vulnerability scan

D. Credentialed scan

Correct Answer: B

A discovery scan is typically used to identify the scope of a web application and understand where the scan will go. This type of scan is often the first step in assessing a web application\\'s security and helps the analyst determine which areas

should be further examined or tested in-depth.

Reference: https://qualysguard.qg2.apps.qualys.com/portal-help/en/was/scans/scanning_basics.htm

QUESTION 3

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:

1.

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

2.

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.

3.

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

The solution will address the findings that the development team used a new software language that was not supported by the security team\\'s automated assessment tools and the security assessment team was unfamiliar with the new language and struggled to evaluate the software during advanced testing. The training of the security assessment team and working with the automated assessmenttool vendor to add support for the new language will ensure that future deployments of the new technology are secure and the vulnerabilities are detected and prevented.

QUESTION 4

During an incident, a security analyst discovers a large amount of PII has been emailed externally from an employee to a public email address. The analyst finds that the external email is the employee\\'s personal email.

Which of the following should the analyst recommend be done first?

A. Place a legal hold on the employee\\'s mailbox.

B. Enable filtering on the web proxy.

C. Disable the public email access with CASB.

D. Configure a deny rule on the firewall.

Correct Answer: A

Placing a legal hold on the employee\\'s mailbox is the best action to perform first, as it preserves all mailbox content, including deleted items and original versions of modified items, for potential legal or forensic purposes. A legal hold is a feature that allows an administrator to retain mailbox data for a user indefinitely or for a specified period, regardless of the user\\'s actions or retention policies. A legal hold can be applied to a mailbox using Litigation Hold or In-Place Hold in Exchange Server or Exchange Online. A legal hold can help to ensure that evidence of data exfiltration or other malicious activities is not lost or tampered with, and that the organization can comply with any legal or regulatory obligations. The other actions are not as urgent or effective as placing a legal hold on the employee\\'s mailbox, as they do not address the immediate threat of data loss or compromise. Enabling filtering on the web proxy may help to prevent some types of data exfiltration or malicious traffic, but it does not help to recover or preserve the data that has already been emailed externally. Disabling the public email access with CASB (Cloud Access Security Broker) may help to block or monitor the use of public email services by employees, but it does not help to recover or preserve the data that has already been emailed externally. Configuring a deny rule on the firewall may help to block or monitor the network traffic from the employee\\'s laptop, but it does not help to recover or preserve the data that has already been emailed externally.

QUESTION 5

An analyst is reviewing a vulnerability report for a server environment with the following entries: Which of the following systems should be prioritized for patching first?

Vulnerability	Severity	CVSS v3	Host IP	Crown jewel	Exploit available
EOL/Obsolete Log4j v1 x	5	-	54.73.224.15	No	No
EOL/Obsolete Log4j v1 x	5	-	54.73.225.17	Yes	No
EOL/Obsolete Log4j v1 x	5	-	10.101.27.98	Yes	No
Microsoft Windows Security Update	4	8.2	10.100.10.52	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.228	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.228	Yes	Yes
Oracle Java Critical Patch	3	6.9	10.101.25.65	Yes	No
Oracle Java Critical Patch	3	6.9	54.73.225.17	Yes	No
Oracle Java Critical Patch	3	6.9	10.101.27.98	Yes	No

A. 10.101.27.98

B. 54.73.225.17

C. 54.74.110.26

D. 54.74.110.228

Correct Answer: D

The system that should be prioritized for patching first is 54.74.110.228, as it has the highest number and severity of vulnerabilities among the four systems listed in the vulnerability report. According to the report, this system has 12 vulnerabilities, with 8 critical, 3 high, and 1 medium severity ratings. The critical vulnerabilities include CVE-2019-0708 (BlueKeep), CVE-2019-1182 (DejaBlue), CVE-2017- 0144 (EternalBlue), and CVE-2017-0145 (EternalRomance), which are all remote code execution vulnerabilities that can allow an attacker to compromise the system without any user interaction or authentication. These vulnerabilities pose a high risk to the system and should be patched as soon as possible.