# 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.passapply.com/cs0-003.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

A security operations manager wants to build out an internal threat-hunting capability. Which of the following should be the first priority when creating a threat-hunting program?

A. Establishing a hypothesis about which threats are targeting which systems

B. Profiling common threat actors and activities to create a list of IOCs

C. Ensuring logs are sent to a centralized location with search and filtering capabilities

D. Identifying critical assets that will be used to establish targets for threat-hunting activities

Correct Answer: C

By aggregating logs in a centralized location with search and filtering capabilities, security analysts can quickly and easily identify anomalous behavior that may indicate a potential threat. Additionally, a centralized location makes it easier to correlate events across multiple systems and identify patterns that may be indicative of an attack.

**QUESTION 2**

An organization has activated the CSIRT. A security analyst believes a single virtual server was compromised and immediately isolated from the network. Which of the following should the CSIRT conduct next? A Take a snapshot of the compromised server and verify its integrity

A. Restore the affected server to remove any malware

B. Contact the appropriate government agency to investigate

C. Research the malware strain to perform attribution

Correct Answer: A

The next action that the CSIRT should conduct after isolating the compromised server from the network is to take a snapshot of the compromised server and verify its integrity. Taking a snapshot of the compromised server involves creating an exact copy or image" specific point in time. Verifying its integrity involves ensuring that the snapshot has not been altered, corrupted, or tampered with during or after its creation. Taking a snapshot and verifying its integrity can help preserve and protect any evidence or information related to the incident, as well as prevent any tampering, contamination, or destruction of evidence.

**QUESTION 3**

The analyst reviews the following endpoint log entry: Which of the following has occurred?

```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator
-ScriptBlock {HOSTName} clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator
-ScriptBlock {net user /add invoke_u1}
The command completed successfully.
```

A. Registry change

B. Rename computer

C. New account introduced

D. Privilege escalation

Correct Answer: C

The endpoint log entry shows that a new account named “admin” has been created on a Windows system with a local group membership of “Administrators”.

This indicates that a new account has been introduced on the system with administrative privileges. This could be a sign of malicious activity, such as privilege escalation or backdoor creation, by an attacker who has compromised the system.

---

**QUESTION 4**

Which of the following software assessment methods world peak times?

A. Security regression testing

B. Stress testing

C. Static analysis testing

D. Dynamic analysis testing

E. User acceptance testing

Correct Answer: B

Stress testing is a software assessment method that tests how an application performs under peak times or extreme workloads. Stress testing can help to identify any performance issues, bottlenecks, errors or crashes that may occur when an application faces high demand or concurrent users. Stress testing can also help to determine the maximum capacity and scalability of an application . https://www.techopedia.com/definition39/memory-dump

---

**QUESTION 5**

An incident response team finished responding to a significant security incident. The management team has asked the lead analyst to provide an after-action report that includes lessons learned. Which of the following is the most likely reason to include lessons learned?

A. To satisfy regulatory requirements for incident reporting

B. To hold other departments accountable

C. To identify areas of improvement in the incident response process

D. To highlight the notable practices of the organization\\'s incident response team

Correct Answer: C

The most likely reason to include lessons learned in an after-action report is to identify areas of improvement in the incident response process. The lessons learned process is a way of reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying areas of improvement in the incident response process can help enhance the security posture, readiness, or capability of the organization for future incidents, as well as provide feedback or recommendations on how to address any issues or challenges.