



# CS0-003<sup>Q&As</sup>

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

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





### QUESTION 1

An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

- A. Disable the user's network account and access to web resources.
- B. Make a copy of the files as a backup on the server.
- C. Place a legal hold on the device and the user's network share.
- D. Make a forensic image of the device and create a SHA-1 hash.

Correct Answer: D

Making a forensic image of the device and creating a SRA-1 hash is the best step to preserve evidence, as it creates an exact copy of the device's data and verifies its integrity. A forensic image is a bit-by-bit copy of the device's storage

media, which preserves all the information on the device, including deleted or hidden files. A SRA-I hash is a cryptographic value that is calculated from the forensic image, which can be used to prove that the image has not been altered or

tampered with. The other options are not as effective as making a forensic image and creating a SRA-1 hash, as they may not capture all the relevant data, or they may not provide sufficient verification of the evidence's authenticity.

<https://www.sans.org/blog/forensics-101-acquiring-an-image-with-ftk-imager/>

<https://swailescomputerforensics.com/digital-forensics-imaging-hash-value/>

---

### QUESTION 2

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 3



A penetration tester submitted data to a form in a web application, which enabled the penetration tester to retrieve user credentials. Which of the following should be recommended for remediation of this application vulnerability?

- A. Implementing multifactor authentication on the server OS
- B. Hashing user passwords on the web application
- C. Performing input validation before allowing submission
- D. Segmenting the network between the users and the web server

Correct Answer: C

Input validation is a critical security measure to prevent various types of web application attacks, including SQL injection, cross-site scripting (XSS), and data manipulation. It helps ensure that user inputs are sanitized and do not contain malicious or unexpected data.

---

#### QUESTION 4

A security analyst needs to ensure that systems across the organization are protected based on the sensitivity of the content each system hosts. The analyst is working with the respective system owners to help determine the best methodology that seeks to promote confidentiality, availability, and integrity of the data being hosted. Which of the following should the security analyst perform first to categorize and prioritize the respective systems?

- A. Interview the users who access these systems.
- B. Scan the systems to see which vulnerabilities currently exist.
- C. Configure alerts for vendor-specific zero-day exploits.
- D. Determine the asset value of each system.

Correct Answer: D

Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data. Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

---

#### QUESTION 5

The security operations team is required to consolidate several threat intelligence feeds due to redundant tools and portals. Which of the following will best achieve the goal and maximize results?

- A. Single pane of glass



- B. Single sign-on
- C. Data enrichment
- D. Deduplication

Correct Answer: D

Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

[CS0-003 PDF Dumps](#)

[CS0-003 Practice Test](#)

[CS0-003 Braindumps](#)