



CS0-002^{Q&As}

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

<https://www.geekcert.com/cs0-002.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 is moving from the use of web servers hosted in an internal datacenter to a containerized cloud platform. An analyst has been asked to identify indicators of compromise in the containerized environment. Which of the following would BEST indicate a running container has been compromised?

- A. A container from an approved software image has drifted
- B. An approved software orchestration container is running with root privileges
- C. A container from an approved software image has stopped responding
- D. A container from an approved software image fails to start

Correct Answer: A

QUESTION 2

An analyst is responding to an incident within a cloud infrastructure. Based on the logs and traffic analysis, the analyst thinks a container has been compromised.

Which of the following should the analyst do FIRST?

- A. Perform threat hunting in other areas of the cloud infrastructure
- B. Contact law enforcement to report the incident
- C. Perform a root cause analysis on the container and the service logs
- D. Isolate the container from production using a predefined policy template

Correct Answer: D

QUESTION 3

A security analyst is investigating a system compromise. The analyst verifies the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely exploited?

- A. Insider threat
- B. Buffer overflow
- C. Advanced persistent threat
- D. Zero day

Correct Answer: D

**QUESTION 4**

An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive?

- A. Reports show the scanner compliance plug-in is out-of-date.
- B. Any items labeled 'low' are considered informational only.
- C. The scan result version is different from the automated asset inventory.
- D. 'HTTPS' entries indicate the web page is encrypted securely.

Correct Answer: B

QUESTION 5

An organization needs to limit its exposure to accidental disclosure when employees send emails that contain personal information to recipients outside the company

Which of the following technical controls would BEST accomplish this goal?

- A. DLP
- B. Encryption
- C. Data masking
- D. SPF

Correct Answer: A

[CS0-002 PDF Dumps](#)

[CS0-002 Study Guide](#)

[CS0-002 Braindumps](#)