



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 cybersecurity analyst was hired to resolve a security issue within a company after it was reported that many employee account passwords had been compromised. Upon investigating the incident, the cybersecurity analyst found that a brute

force attack was launched against the company.

Which of the following remediation actions should the cybersecurity analyst recommend to senior management to address these security issues?

- A. Prohibit password reuse using a GPO.
- B. Deploy multifactor authentication.
- C. Require security awareness training.
- D. Implement DLP solution.

Correct Answer: B

QUESTION 2

Which of the following organizational initiatives would be MOST impacted by data severignty issues?

- A. Moving to a cloud-based environment
- B. Migrating to locally hosted virtual servers
- C. Implementing non-repudiation controls
- D. Encrypting local database queries

Correct Answer: A

QUESTION 3

Massivelog.log has grown to 40GB on a Windows server. At this size, local tools are unable to read the file, and it cannot be moved off the virtual server where it is located.

Which of the following lines of PowerShell script will allow a user to extract the last 10,000 lines of the log for review?

- A. `tail -10000 Massivelog.log > extract.txt`
- B. `info tail n -10000 Massivelog.log | extract.txt;`
- C. `get content `./Massivelog.log\` -Last 10000 | extract.txt`
- D. `get-content `./Massivelog.log\` -Last 10000 > extract.txt;`

Correct Answer: D



QUESTION 4

In the development stage of the incident response policy, the security analyst needs to determine the stakeholders for the policy. Who of the following would be the policy stakeholders?

- A. Human resources, legal, public relations, management
- B. Chief information Officer (CIO), Chief Executive Officer, board of directors, stockholders
- C. IT, human resources, security administrator, finance
- D. Public information officer, human resources, audit, customer service

Correct Answer: B

QUESTION 5

A security analyst was asked to join an outage call for a critical web application. The web middleware support team determined the web server is running and having no trouble processing requests; however, some investigation has revealed firewall denies to the web server that began around 1.00 a.m. that morning. An emergency change was made to enable the access, but management has asked for a root cause determination. Which of the following would be the BEST next step?

- A. Install a packet analyzer near the web server to capture sample traffic to find anomalies.
- B. Block all traffic to the web server with an ACL.
- C. Use a port scanner to determine all listening ports on the web server.
- D. Search the logging servers for any rule changes.

Correct Answer: D

[Latest CS0-002 Dumps](#)

[CS0-002 PDF Dumps](#)

[CS0-002 Braindumps](#)