



Visit and Download Full Version Certificationtime Exam Dumps
<https://certificationtime.com/updated/cs0-001-exam-dumps-pdf/>

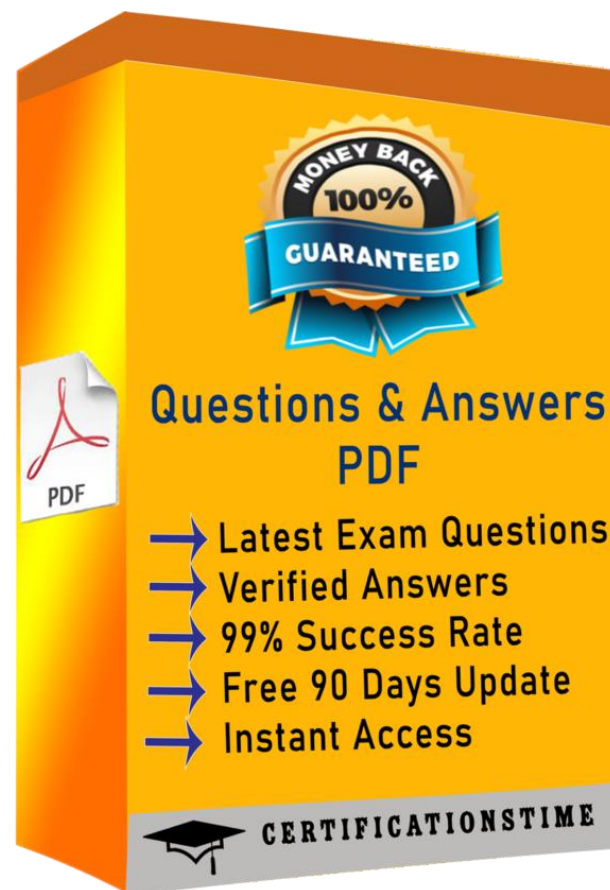


CompTIA

Exam Questions CS0-001

CompTIA CSA+ Certification Exam

<https://certificationtime.com/>





Question: 1

Which of the following BEST describes the offensive participants in a tabletop exercise?

- A. Red team
- B. Blue team
- C. System administrators
- D. Security analysts
- E. Operations team

Answer: A

Question: 2

After analyzing and correlating activity from multiple sensors, the security analyst has determined a group from a high-risk country is responsible for a sophisticated breach of the company network and continuous administration of targeted attacks for the past three months. Until now, the attacks went unnoticed. This is an example of:

- A. privilege escalation.
- B. advanced persistent threat.
- C. malicious insider threat.
- D. spear phishing.

Answer: B

Question: 3

A system administrator who was using an account with elevated privileges deleted a large amount of log files generated by a virtual hypervisor in order to free up disk space. These log files are needed by the security team to analyze the health of the virtual machines. Which of the following compensating controls would help prevent this from reoccurring? (Select two.)

- A. Succession planning
- B. Separation of duties
- C. Mandatory vacation
- D. Personnel training

Questions & Answers PDF Page 5

<https://certificationtime.com/updated/cs0-001-exam-dumps-pdf/>

- E. Job rotation

Answer: B,D

Question: 4

Which of the following best practices is used to identify areas in the network that may be vulnerable to penetration testing from known external sources?

- A. Blue team training exercises
- B. Technical control reviews
- C. White team training exercises
- D. Operational control reviews

Answer: A

Question: 5

An organization has recently recovered from an incident where a managed switch had been accessed and reconfigured without authorization by an insider. The incident response team is working on developing a lessons learned report with recommendations. Which of the following recommendations will BEST prevent the same attack from occurring in the future?

- A. Remove and replace the managed switch with an unmanaged one.
- B. Implement a separate logical network segment for management interfaces.
- C. Install and configure NAC services to allow only authorized devices to connect to the network.
- D. Analyze normal behavior on the network and configure the IDS to alert on deviations from normal.

Answer: B



Question: 6

A cybersecurity analyst is reviewing the current BYOD security posture. The users must be able to synchronize their calendars, email, and contacts to a smartphone or other personal device. The recommendation must provide the most flexibility to users. Which of the following recommendations would meet both the mobile data protection efforts and the business requirements described in this scenario?

- A. Develop a minimum security baseline while restricting the type of data that can be accessed.
- B. Implement a single computer configured with USB access and monitored by sensors.
- C. Deploy a kiosk for synchronizing while using an access list of approved users.
- D. Implement a wireless network configured for mobile device access and monitored by sensors.

Answer: D

Question: 7

Questions & Answers PDF Page 6

A security analyst received a compromised workstation. The workstation's hard drive may contain evidence of criminal activities. Which of the following is the FIRST thing the analyst must do to ensure the integrity of the hard drive while performing the analysis?

- A. Make a copy of the hard drive.
- B. Use write blockers.
- C. Run `rm -R` command to create a hash.
- D. Install it on a different machine and explore the content.

Answer: B

Full Access:

<https://certificationtime.com/updated/cs0-001-exam-dumps-pdf/>