



GCCC^{Q&As}

GCCC - GIAC Critical Controls Certification (GCCC)

Pass GIAC GCCC Exam with 100% Guarantee

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

<https://www.geekcert.com/gcc.html>

100% Passing Guarantee
100% Money Back Assurance

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

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





QUESTION 1

Janice is auditing the perimeter of the network at Sugar Water InC. According to documentation, external SMTP traffic is only allowed to and from 10.10.10.25. Which of the following actions would demonstrate the rules are configured incorrectly?

- A. Receive spam from a known bad domain
- B. Receive mail at Sugar Water Inc. account using Outlook as a mail client
- C. Successfully deliver mail from another host inside the network directly to an external contact
- D. Successfully deliver mail from web client using another host inside the network to an external contact.

Correct Answer: C

QUESTION 2

A need has been identified to organize and control access to different classifications of information stored on a fileserver. Which of the following approaches will meet this need?

- A. Organize files according to the user that created them and allow the user to determine permissions
- B. Divide the documents into confidential, internal, and public folders, and set permissions on each folder
- C. Set user roles by job or position, and create permission by role for each file
- D. Divide the documents by department and set permissions on each departmental folder

Correct Answer: B

QUESTION 3

An organization is implementing an application software security control their custom-written code that provides web--based database access to sales partners. Which action will help mitigate the risk of the application being compromised?

- A. Providing the source code for their web application to existing sales partners
- B. Identifying high-risk assets that are on the same network as the web application server
- C. Creating signatures for their IDS to detect attacks specific to their web application
- D. Logging the connection requests to the web application server from outside hosts

Correct Answer: C

QUESTION 4



Beta corporation is doing a core evaluation of its centralized logging capabilities. The security staff suspects that the central server has several log files over the past few weeks that have had their contents changed. Given this concern, and the need to keep archived logs for log correction applications, what is the most appropriate next steps?

- A. Keep the files in the log archives synchronized with another location.
- B. Store the files read-only and keep hashes of the logs separately.
- C. Install a tier one timeserver on the network to keep log devices synchronized.
- D. Encrypt the log files with an asymmetric key and remove the cleartext version.

Correct Answer: B

QUESTION 5

An organization has failed a test for compliance with a policy of continual detection and removal of malicious software on its network. Which of the following errors is the root cause?

- A. A host ran malicious software that exploited a vulnerability for which there was no patch
- B. The security console alerted when a host anti-virus ran whitelisted software
- C. The intrusion prevention system failed to update to the newest signature list
- D. A newly discovered vulnerability was not detected by the intrusion detection system

Correct Answer: C

[GCCC PDF Dumps](#)

[GCCC VCE Dumps](#)

[GCCC Study Guide](#)