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.passapply.com/gccc.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

Which of the following is necessary to automate a control for Inventory and Control of Hardware Assets?

A. A method of device scanning

B. A centralized time server

C. An up-to-date hardening guide

D. An inventory of unauthorized assets

Correct Answer: A

QUESTION 2

Acme Corporation performed an investigation of its centralized logging capabilities. It found that the central server is missing several types of logs from three servers in Acme\\'s inventory. Given these findings, what is the most appropriate next step?

A. Define processes to manually review logs for the problem servers

B. Restart or reinstall the logging service on each of the problem servers

C. Perform analysis to identify the source of the logging problems

D. Document the missing logs in the core evaluation report as a minor issue

Correct Answer: C

QUESTION 3

A security incident investigation identified the following modified version of a legitimate system file on a compromised client:

C:\Windows\System32\winxml.dll Addition Jan. 16, 2014 4:53:11 PM

The infection vector was determined to be a vulnerable browser plug-in installed by the user. Which of the organization\\'s CIS Controls failed?

A. Application Software Security

B. Inventory and Control of Software Assets

C. Maintenance, Monitoring, and Analysis of Audit Logs

D. Inventory and Control of Hardware Assets

Correct Answer: B

QUESTION 4

Which of the following should be used to test antivirus software?

A. FIPS 140-2

B. Code Red

C. Heartbleed

D. EICAR

Correct Answer: D

QUESTION 5

An analyst investigated unused organizational accounts. The investigation found that:

-10% of accounts still have their initial login password, indicating they were never used

-10% of accounts have not been used in over six months

Which change in policy would mitigate the security risk associated with both findings?

A. Users are required to change their password at the next login after three months

B. Accounts must have passwords of at least 8 characters, with one number or symbol

C. Accounts without login activity for 15 days are automatically locked

Correct Answer: C