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/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

Acme Corporation is doing a core evaluation of its centralized logging capabilities. Which of the following scenarios indicates a failure in more than one CIS Control?

A. The loghost is missing logs from 3 servers in the inventory

B. The loghost is receiving logs from hosts with different timezone values

C. The loghost time is out-of-sync with an external host

D. The loghost is receiving out-of-sync logs from undocumented servers

Correct Answer: D

QUESTION 2

An organization has implemented a policy to continually detect and remove malware from its network. Which of the following is a detective control needed for this?

A. Host-based firewall sends alerts when packets are sent to a closed port

B. Network Intrusion Prevention sends alerts when RST packets are received

C. Network Intrusion Detection devices sends alerts when signatures are updated

D. Host-based anti-virus sends alerts to a central security console

Correct Answer: D

QUESTION 3

An auditor is validating the policies and procedures for an organization with respect to a control for Data Recovery. The organization\\'s control states they will completely back up critical servers weekly, with incremental backups every four hours. Which action will best verify success of the policy?

A. Verify that the backup media cannot be read without the encryption key

B. Check the backup logs from the critical servers and verify there are no errors

C. Select a random file from a critical server and verify it is present in a backup set

D. Restore the critical server data from backup and see if data is missing

Correct Answer: D

QUESTION 4

Dragonfly Industries requires firewall rules to go through a change management system before they are configured.

Review the change management log. Which of the following lines in your firewall ruleset has expired and should be removed from the configuration?

Line	Date	Port	Internal Host(s)	External Host(s)	In/Out/Both	Length rule is needed	Reason
1	1/15/2013	22	8.8.207.97	10.10.12.100	in	6 weeks	software set-up
2	5/12/2013	25	10.1.1.7	any	out	indefinite	marketing mail delivery
3	6/17/2013	8080	10.10.12.252	8.8.0.0/24	in	indefinite	network backup transfers
4	10/21/2013	80	any	74.125.228.2	out	indefinite	prevent video browsing
5	4/4/2014	443	10.10.12.17	any	in	indefinite	enable secure access

A. access-list outbound permit tcp host 10.1.1.7 any eq smtp

B. access-list outbound deny tcp any host 74.125.228.2 eq www

C. access-list inbound permit tcp 8.8.0.0 0.0.0.255 10.10.12.252 eq 8080

D. access-list inbound permit tcp host 8.8.207.97 host 10.10.12.100 eq ssh

Correct Answer: D

QUESTION 5

What is a zero-day attack?

A. An attack that has a known attack signature but no available patch

B. An attack that utilizes a vulnerability unknown to the software developer

C. An attack that deploys at the end of a countdown sequence

D. An attack that is launched the day the patch is released

Correct Answer: B