ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: GIAC

Code: GCCC

Exam: GIAC Critical Controls Certification

https://www.examsnest.com/exam/gccc/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 4.0

Question: 1

An organization has implemented a policy to detect and remove malicious software from its network. Which of the following actions is focused on correcting rather than preventing attack?

A. Configuring a firewall to only allow communication to whitelisted hosts and ports
B. Using Network access control to disable communication by hosts with viruses
C. Disabling autorun features on all workstations on the network
D. Training users to recognize potential phishing attempts

Answer: B

Question: 2

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.

Answer: B

Question: 3

Which projects enumerates or maps security issues to CVE?

A. SCAP
B. CIS Controls
C. NIST
D. ISO 2700

Answer: A

Question: 4

Which of the following archiving methods would maximize log integrity?

A. DVD-R
B. USB flash drive
C. Magnetic Tape
D. CD-RW

Answer: A

Question: 5

Which of the following is a responsibility of a change management board?

A. Reviewing log files for unapproved changes
B. Approving system baseline configurations.
C. Providing recommendations for the changes
D. Reviewing configuration of the documents

Answer: B

Question: 6

Which of the following is a benefit of stress-testing a network?

A. To determine device behavior in a DoS condition.
B. To determine bandwidth needs for the network.
C. To determine the connectivity of the network
D. To determine the security configurations of the network

Answer: A

Question: 7

An organization has implemented a control for Controlled Use of Administrative Privilege. The control requires users to enter a password from their own user account before being allowed elevated privileges, and that no client applications (e.g. web browsers, e-mail clients) can be run with elevated privileges. Which of the following actions will validate this control is implemented properly?

A. Check the log entries to match privilege use with access from authorized users.
B. Run a script at intervals to identify processes running with administrative privilege.
C. Force the root account to only be accessible from the system console.

Answer: B

Question: 8

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

Answer: B

Question: 9

An organization is implementing a control for the Account Monitoring and Control CIS Control, and have set the Account Lockout Policy as shown below. What is the risk presented by these settings?

(Image)

A. Brute-force password attacks could be more effective.
B. Legitimate users could be unable to access resources.
C. Password length and complexity will be automatically reduced.
D. Once accounts are locked, they cannot be unlocked.

Answer: B

Question: 10

An organization has implemented a control for Controlled Use of Administrative Privileges. They are collecting audit data for each login, logout, and location for the root account of their MySQL server, but they are unable to attribute each of these logins to a specific user. What action can they take to rectify this?

A. Force the root account to only be accessible from the system console.
B. Turn on SELinux and user process accounting for the MySQL server.
C. Force user accounts to use 'sudo' f or privileged use.
D. Blacklist client applications from being run in privileged mode.

Answer: C

Question: 11

What type of Unified Modelling Language (UML) diagram is used to show dependencies between logical groupings in a system?

A. Package diagram
B. Deployment diagram
C. Class diagram
D. Use case diagram

Answer: A

Question: 12

IDS alerts at Service Industries are received by email. A typical day process over 300 emails with fewer than 50 requiring action. A recent attack was successful and went unnoticed due to the number of generated alerts. What should be done to prevent this from recurring?

A. Tune the IDS rules to decrease false positives.
B. Increase the number of staff responsible for processing IDS alerts.
C. Change the alert method from email to text message.
D. Configure the IDS alerts to only alert on high priority systems.

Answer: A

Question: 13

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.

Answer: C

Question: 14

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

A. FIPS 140-2

B. Code Red
C. Heartbleed
D. EICAR

Answer: D

ExamsNest
Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: GIAC

Code: GCCC

Exam: GIAC Critical Controls Certification

https://www.examsnest.com/exam/gccc/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation