# 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**

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 2**

An organization is implementing a control within the Application Software Security CIS Control. How can they best protect against injection attacks against their custom web application and database applications?

A. Ensure the web application server logs are going to a central log host

B. Filter input to only allow safe characters and strings

C. Configure the web server to use Unicode characters only

D. Check user input against a list of reserved database terms

Correct Answer: B

**QUESTION 3**

A breach was discovered after several customers reported fraudulent charges on their accounts. The attacker had exported customer logins and cracked passwords that were hashed but not salted. Customers were made to reset their passwords.

Shortly after the systems were cleaned and restored to service, it was discovered that a compromised system administrator\\'s account was being used to give the attacker continued access to the network. Which CIS Control failed in the continued access to the network?

A. Maintenance, Monitoring, and Analysis of Audit Logs

B. Controlled Use of Administrative Privilege

C. Incident Response and Management

D. Account Monitoring and Control

Correct Answer: C

**QUESTION 4**

Which of the following best describes the CIS Controls?

A. Technical, administrative, and policy controls based on research provided by the SANS Institute

B. Technical controls designed to provide protection from the most damaging attacks based on current threat data

C. Technical controls designed to augment the NIST 800 series

D. Technical, administrative, and policy controls based on current regulations and security best practices

Correct Answer: B

**QUESTION 5**

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