# GCED Q&As

GIAC Certified Enterprise Defender Practice Test

## Pass GIAC GCED Exam with 100% Guarantee

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

**https://www.pass2lead.com/gced.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**

An incident response team is handling a worm infection among their user workstations. They created an

IPS signature to detect and block worm activity on the border IPS, then removed the worm\\'s artifacts or

workstations triggering the rule.

Despite this action, worm activity continued for days after. Where did the incident response team fail?

A. The team did not adequately apply lessons learned from the incident

B. The custom rule did not detect all infected workstations

C. They did not receive timely notification of the security event

D. The team did not understand the worm\\'s propagation method

Correct Answer: B

Explanation: Identifying and scoping an incident during triage is important to successfully handling a security incident. The detection methods used by the team didn\\'t detect all the infected workstations.

**QUESTION 2**

A company classifies data using document footers, labeling each file with security labels "Public", "Pattern", or "Company Proprietary". A new policy forbids sending "Company Proprietary" files via email. Which control could help security analysis identify breaches of this policy?

A. Monitoring failed authentications on a central logging device

B. Enforcing TLS encryption for outbound email with attachments

C. Blocking email attachments that match the hashes of the company\\'s classification templates

D. Running custom keyword scans on outbound SMTP traffic from the mail server

Correct Answer: D

**QUESTION 3**

A company wants to allow only company-issued devices to attach to the wired and wireless networks. Additionally, devices that are not up-to-date with OS patches need to be isolated from the rest of the network until they are updated. Which technology standards or protocols would meet these requirements?

A. 802.1x and Network Access Control

B. Kerberos and Network Access Control

C. LDAP and Authentication, Authorization and Accounting (AAA)

D. 802.11i and Authentication, Authorization and Accounting (AAA)

Correct Answer: A

**QUESTION 4**

Which Windows CLI tool can identify the command-line options being passed to a program at startup?

A. netstat

B. attrib

C. WMIC

D. Tasklist

Correct Answer: C

**QUESTION 5**

What are Browser Helper Objects (BHO)s used for?

A. To provide multi-factor authentication support for Firefox

B. To provide a more feature-rich interface for Internet Explorer

C. To allow Internet Explorer to process multi-part URLs

D. To allow Firefox to process JavaScript in a sandbox

Correct Answer: B

Explanation: When scanning your system, you may notice many BHOs since they are widely used by software developers to provide a more feature rich interface for Microsoft Internet Explorer.