

**Boost up Your Certification Score**

# **GIAC GEIR**

**GIAC Enterprise Incident Response**



**For More Information – Visit link below:**

**<https://www.examsboost.com/>**

## **Product Version**

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

Visit us at: <https://www.examsboost.com/test/geir>

# Latest Version: 6.0

## Question: 1

What are effective practices for maintaining enterprise visibility to support incident scoping?  
Response:

- A. Regular data purging to free up storage space
- B. Continuous monitoring of network traffic
- C. Integrating SIEM solutions for real-time analysis
- D. Periodic manual audits of security settings

**Answer: B,C**

## Question: 2

The default location for system log files in a Linux system is \_\_\_\_\_.  
Response:

- A. /var/log
- B. /etc/log
- C. /usr/log
- D. /home/log

**Answer: A**

## Question: 3

What is the FIRST step an incident responder should take after identifying an anomaly that could indicate a modern attack?  
Response:

- A. Notify all company employees about the anomaly
- B. Isolate the affected system from the network
- C. Collect and preserve digital evidence
- D. Perform a full system backup

**Answer: C**

### Question: 4

In the context of rapid response triage at scale, which macOS features assist in remote incident handling?

(Choose Three)

Response:

- A. Remote Desktop
- B. Time Machine
- C. Terminal
- D. System Preferences
- E. Screen Sharing

**Answer: A,C,E**

### Question: 5

Which of the following are essential tools for malware analysis on macOS?

(Choose Two)

Response:

- A. Terminal
- B. Keychain Access
- C. Activity Monitor
- D. Finder

**Answer: A,C**

### Question: 6

For analyzing log data effectively, which command is best suited for sorting and extracting specific information?

Response:

- A. cat
- B. grep
- C. touch
- D. chmod

**Answer: B**

### Question: 7

Select the macOS features that assist in recovery and backup.

(Multiple Correct Answers)

Response:

- A. Time Machine
- B. Disk Utility
- C. Finder
- D. Boot Camp
- E. Spotlight

**Answer: A,B**

### Question: 8

In a cloud-based incident response, which tool is commonly used to analyze network traffic to and from a cloud environment?

Response:

- A. Wireshark
- B. Splunk
- C. Microsoft Excel
- D. Adobe Acrobat

**Answer: A**

### Question: 9

What capabilities should a tool have to effectively collect and process incident response data at scale across macOS endpoints?

(Choose Three)

Response:

- A. Remote script execution
- B. Automatic user logout
- C. Network traffic monitoring
- D. Live memory analysis
- E. System log aggregation

**Answer: A,D,E**

## Question: 10

Which tool is primarily used for detailed investigation of the filesystem in Linux DFIR tasks?  
Response:

- A. Grep
- B. Sed
- C. Awk
- D. Debugfs

**Answer: D**

# Thank You for Trying Our Product

For More Information – **Visit link below:**

**<https://www.examsboost.com/>**

15 USD Discount Coupon Code:

**G74JA8UF**

## FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/geir>