

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

Which protocol is used by macOS for system-wide logging and how is it accessed?

Response:

- A. Syslog, accessed through Console
- B. ASL, accessed through Console
- C. NFS, accessed through System Preferences
- D. SMB, accessed through Terminal

Answer: B

Question: 2

Which tool is commonly used for monitoring and managing containerized applications?

Response:

- A. Docker
- B. Wireshark
- C. Metasploit
- D. Nessus

Answer: A

Question: 3

What is the primary purpose of the macOS Keychain application?

Response:

- A. Monitor system performance
- B. Manage passwords and encryption keys
- C. Configure network settings
- D. Install and update software

Answer: B

Question: 4

Which of the following are common data sources in an enterprise environment that can aid in incident scoping?

Response:

- A. HR management systems
- B. Network flow data
- C. Antivirus logs
- D. Application logs
- E. Email transaction logs

Answer: B,C,D,E

Question: 5

Which of the following telemetry sources are critical for scoping incidents related to unauthorized data access?

Response:

- A. Database access logs
- B. Print server logs
- C. IDS/IPS alerts
- D. File integrity monitoring systems
- E. Network configuration changes

Answer: A,C,D

Question: 6

What is an essential element when developing a playbook for managing ransomware attacks in an enterprise?

Response:

- A. Legal advice on negotiating ransom payments
- B. Guidelines for isolation, identification of the attack vector, and system restoration
- C. Instructions for paying the ransom quickly to minimize downtime
- D. Procedures for immediate full system backups during an attack

Answer: B

Question: 7

In Linux, user account information is stored in the _____ file.

Response:

- A. /etc/passwd
- B. /etc/users
- C. /etc/accounts
- D. /etc/people

Answer: A

Question: 8

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: 9

What is the default directory for system logs in macOS?

Response:

- A. /var/logs
- B. /etc/logs
- C. /Library/Logs
- D. /System/Logs

Answer: C

Question: 10

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

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>