Congratulations! You passed!

Grade received 81.25%

Latest Submission Grade 81.25%

To pass 80% or higher

Go to next item

Weekly challenge 3

Quiz • 40 min

Review Learning Objectives

1. Which of the following statements correctly describe logs? Select three answers. **0.75 / 1 point**

Outbound requests to the internet from within a network are recorded in a firewall log.

Correct

Security teams monitor logs to identify vulnerabilities and potential data breaches.

Correct

Connections between devices and services on a network are recorded in a firewall log.

This should not be selected
Please review the video on logs and SIEM tools.

Actions such as login requests are recorded in a server log.

Correct

2. What are some of the key benefits of SIEM tools? Select three answers. **0.75 / 1 point**

Provide visibility

Correct

Automatic updates customized to new threats and vulnerabilities

This should not be selected
Please review the video on logs and SIEM tools.

Monitor critical activities in an organization

Correct

Store all log data in a centralized location

Correct

3. Fill in the blank: To assess the performance of a software application, security professionals use _____, including response time, availability, and failure rate. **1 / 1 point**

- logs
- SIEM tools
- dashboards
- metrics

Correct

4. A security team chooses to implement a SIEM tool that they will install, operate, and maintain using their own physical infrastructure. What type of tool are they using? **1 / 1 point**

- Hybrid
- Log-hosted
- Self-hosted
- Cloud-hosted

Correct

5. You are a security analyst, and you want a security solution that will be fully maintained and managed by your SIEM tool provider. What type of tool do you choose? **1 / 1 point**

- Cloud-hosted
- Solution-hosted
- Hybrid
- Self-hosted

Correct

6. Fill in the blank: SIEM tools are used to search, analyze, and _____ an organization's log data to provide security information and alerts in real-time. **1 / 1 point**

- release
- retain
- modify
- separate

Correct

7. After receiving an alert about a suspicious login attempt, a security analyst can access their _____ to gather information about the alert. **1 / 1 point**

- playbook
- internal infrastructure
- SIEM tool dashboard
- network protocol analyzer (packet sniffer)

Correct

8. Fill in the blank: The wide exposure and immediate access to the source code of open-source tools makes it _____ likely that issues will occur. **0 / 1 point**

- very
- more
- equally
- less

Incorrect
Please review the reading on cybersecurity tools.

Submit your assignment

Try again

Due Jun 18, 11:59 PM +08 Attempts 3 every 24 hours

Receive grade

To Pass 80% or higher

Your grade
81.25%

View Feedback
We keep your highest score

Like Dislike Report an issue