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**

A record of events related to employee logins and username requests is part of a server log.

Correct

Submit your assignment

Try again

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

SIEM tools rely on logs to monitor systems and detect security threats.

Receive grade

Correct

To Pass 80% or higher

Your grade 81.25%

View Feedback

We keep your highest score

A record of connections between devices and services on a network is part of a network log.

Correct

Like Dislike Report an issue

Actions such as username requests are recorded in a network log.

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

2. What are some of the key benefits of SIEM tools? Select three answers. **0 / 1 point**

Increase efficiency

Correct

Automatic customization to changing security needs

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

Minimize the number of logs to be manually reviewed

Correct

Deliver automated alerts

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**

- (•) metrics
- ( ) dashboards
- ( ) SIEM tools
- ( ) logs

Correct

4. A security team installs a SIEM tool within their company's own infrastructure to keep private data on internal servers. What type of tool are they using? **1 / 1 point**

- ( ) Cloud-hosted
- ( ) Hybrid
- ( ) Infrastructure-hosted
- (•) Self-hosted

Correct

5. You are a security professional, and you want a SIEM tool that will require both on-site infrastructure and internet-based solutions. What type of tool do you choose? **1 / 1 point**

- ( ) Component-hosted
- ( ) Self-hosted
- ( ) Cloud-hosted
- (•) Hybrid

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**

- ( ) separate
- ( ) modify
- ( ) release
- (•) retain

Correct

7. Which tool provides a comprehensive, visual summary of security-related data, including metrics? **1 / 1 point**

- ( ) Playbook
- (•) SIEM
- ( ) network protocol analyzer (packet sniffer)
- ( ) Command-line interface

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**

- ( ) more
- (•) very
- ( ) equally
- ( ) less

Incorrect
Please review the reading on cybersecurity tools.