Congratulations! You passed!

Grade received 100%

Weekly challenge 3

Latest Submission Grade 100%

To pass 80% or higher

Quiz • 40 min

Retake the assignment in **23h 57m**

Go to next item

Review Learning Objectives

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

- [x] SIEM tools rely on logs to monitor systems and detect security threats.

  Correct

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

  Correct

- [ ] Actions such as username requests are recorded in a network log.
- [x] A record of connections between devices and services on a network is part of a network log.

  Correct

Like **Dislike** **Report an issue**

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

- [ ] Automatic customization to changing security needs
- [x] Minimize the number of logs to be manually reviewed

  Correct

- [x] Increase efficiency

  Correct

- [x] Deliver automated alerts

  Correct

3. Fill in the blank: Software application _____ are technical attributes, such as response time, availability, and failure rate. **1 / 1 point**

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

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
- ( ) Cloud-hosted
- ( ) Log-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**

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

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

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**

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

Correct

8. Which type of tool typically requires users to pay for usage? **1 / 1 point**

- (•) Proprietary
- ( ) Self-hosted
- ( ) Open-source
- ( ) Cloud native

Correct

Submit your assignment **Try again**

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

Retake the quiz in **23h 57m**

Receive grade

To Pass 80% or higher

Your grade
100%

View Feedback

We keep your highest score