1. Which of the following statements correctly describe logs? Select three answers. **0.5 / 1 point**

- [x] 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.

- [x] Security teams monitor logs to identify vulnerabilities and potential data breaches.

Correct

- [ ] Outbound requests to the internet from within a network are recorded in a firewall log.
- [x] 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 / 1 point**

- [x] Automatic customization to changing security needs

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

- [x] Increase efficiency

Correct

- [x] Deliver automated alerts

Correct

- [x] Minimize the number of logs to be manually reviewed

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**

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

Correct

4. A security team chooses to implement a SIEM tool that will be managed and maintained by the organization's IT department, rather than a third-party vendor. What type of tool are they using? **1 / 1 point**

- ( ) Hybrid
- ( ) Department-hosted
- ( ) Cloud-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**

- ○ Cloud-hosted
- ○ Self-hosted
- ◉ Hybrid
- ○ Component-hosted

✓ **Correct**

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

- ○ Operating systems
- ◉ SIEM tools
- ○ Playbooks
- ○ network protocol analyzers (packet sniffers)

✓ **Correct**

7. A security analyst receives an alert about hundreds of login attempts from unusual geographic locations within the last few minutes. What can the analyst use to review a timeline of the login attempts, locations, and time of activity? **1 / 1 point**

- ○ An operating system
- ◉ A SIEM tool dashboard
- ○ A playbook
- ○ A network protocol analyzer (packet sniffer)

✓ **Correct**

8. Fill in the blank: _____ tools are often free to use. **1 / 1 point**

- ○ Command-line
- ○ Proprietary
- ◉ Open-source
- ○ Cloud-hosted

✓ **Correct**