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

A log is a record of events that occur within an organization’s systems and networks.
Correct
A network log is a record of all computers and devices that enter and leave a network.
Correct
Events related to websites, emails, or file shares are recorded in a server log.
Correct

Actions such as using a username or password are recorded in a firewall log.

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

Increase efficiency
Correct
Automatic customization to changing security needs
Deliver automated alerts
Correct
Minimize the number of logs to be manually reviewed
Correct

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

SIEM tools
logs
dashboards
metrics

Correct

Question 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

Department-hosted
Cloud-hosted
Hybrid
Self-hosted
Correct

Question 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

Self-hosted
Cloud-hosted
Component-hosted
Hybrid
Correct

Question 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
network protocol analyzers (packet sniffers)
SIEM tools
Playbooks
Correct

Question 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
network protocol analyzer (packet sniffer)
playbook
internal infrastructure
Correct

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

Cloud native
Open-source
Proprietary
Self-hosted
Correct