

1. What tool is designed to capture and analyze data traffic within a network?

1 point

- ☐ security information and event management (SIEM)
- ☐ Structured Query Language (SQL)
- ☒ network protocol analyzer (packet sniffer)
- ☐ playbook

2. What type of tool uses dashboards to organize data into categories and allows analysts to identify potential security incidents as they happen?

1 point

- ☐ network protocol analyzers (packet sniffers)
- ☒ SIEM
- ☐ Python
- ☐ Linux

3. What can cybersecurity professionals use logs for?

1 point

- ☐ To research and optimize processing capabilities within a network
- ☐ To analyze data traffic within a network
- ☐ To select which security team members will respond to an incident
- ☒ To identify vulnerabilities and potential security breaches

4. Fill in the blank: A _____ is a manual that provides details about operational actions.

1 point

- ☐ checklist
- ☒ playbook