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

☑ A business might log errors that occurred as a result of high network traffic.

✓ Correct

□ A log is used as a formal guide to incident response.

☑ Logs help identify vulnerabilities and potential security breaches.

✓ Correct

□ Security professionals use logs to query databases.

2. Which of the following tasks can be performed using SIEM tools? Select three answers. 1 / 1 point

☑ Analyzing filtered events and patterns

✓ Correct

☑ Saving time by reducing the amount of data to be reviewed

✓ Correct

□ Implementing security software programs

☑ Monitoring critical activities

✓ Correct

3. A cybersecurity analyst needs to collect data from multiple places to analyze filtered events and patterns. What type of tool should they use? 1 / 1 point

○ Linux operating system
○ Playbook
○ network protocol analyzer (packet sniffer)
● Security information and event management (SIEM)

✓ Correct

4. Fill in the blank: A security professional uses a _____ as a manual to guide operational activities. 1 / 1 point

● playbook
○ toolkit
○ spreadsheet
○ review

✓ Correct

5. As a security analyst, you are monitoring network traffic to ensure that SPII data is not being accessed by unauthorized users. What does this scenario describe? 1 / 1 point

● Using a network protocol analyzer (packet sniffer)
○ Programming with code
○ Calculating with formulas
○ Gathering data in a spreadsheet

✓ Correct

6. What are some key benefits of programming languages? Select all that apply. 1 / 1 point

☑ They can be used to create a specific set of instructions for a computer to execute tasks.

✓ Correct

☑ They filter through data points faster than humans can working manually.

✓ Correct

☐ They install security hardware.

☑ They execute repetitive processes accurately.

✓ Correct

7. A security team wants to examine logs to understand what is occurring within their systems. Why might they choose Linux to perform this task? Select two answers. 1 / 1 point

☑ It is open source.

✓ Correct

☐ It is proprietary.

☑ It allows for text-based commands by users.

✓ Correct

☐ It is an efficient programming language.

8. Fill in the blank: To request information from a _____, security professionals can use SQL. 1 / 1 point

○ dashboard

○ network

○ spreadsheet

● database

✓ Correct

9. What are some key benefits of using Python to perform security tasks? Select all that apply. 0.5 / 1 point

☑ It simplifies repetitive tasks.

✓ Correct

☑ It helps security professionals be more accurate.

✓ Correct

□ It is designed for high levels of accuracy.