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

- [ ] Security professionals use logs to query databases.
- [x] A business might log errors that occurred as a result of high network traffic.

Correct

- [x] Logs help identify vulnerabilities and potential security breaches.

Correct

- [ ] A log is used as a formal guide to incident response.

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

- [x] Performing incident analysis

Correct

- [x] Proactively searching for threats

Correct

- [ ] Notifying authorities of illegal activity
- [x] Providing alerts for specific types of risks

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? **0 / 1 point**

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

Incorrect
Please review the video on tools.

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

- ( ) spreadsheet
- ( ) toolkit
- ( ) review
- (•) playbook

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 are used to design security policies.
- [x] They can be used to create a specific set of instructions for a computer to execute tasks.

Correct

- [x] They complete tasks faster than if working manually.

Correct

- [x] They reduce the risk of human error.

Correct

7. Fill in the blank: Linux relies on a(n) _____ as the primary user interface. **1 / 1 point**

- (●) command line
- ( ) ciphertext
- ( ) dashboard
- ( ) error log

✓ **Correct**

8. Fill in the blank: Security professionals can use _____ to interact with and request information from a database. **1 / 1 point**

- (●) SQL
- ( ) network protocol analyzers (packet sniffers)
- ( ) logs
- ( ) playbooks

✓ **Correct**

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

- [x] It helps security professionals be more accurate.

✓ **Correct**

- [x] It is designed for high levels of accuracy.

✓ **Correct**

- [x] It simplifies repetitive tasks.

✓ **Correct**

- [ ] It makes static data more dynamic.