

Question 1

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

A business might log each time an employee accesses web-based services.

Correct

Logs helps identify vulnerabilities and potential security breaches.

Correct

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

Security professionals use logs to automate tasks.

Question 2

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

Implementing security software programs

Saving time by reducing the amount of data to be reviewed

Correct

Monitoring critical activities

Correct

Analyzing filtered events and patterns

Correct

Question 3

Fill in the blank: Instead of reviewing pages and pages of logs to determine if there are any new security threats, analysts can use \_\_\_\_\_ tools, which provide alerts for specific types of threats and risks. 1 / 1 point

security information and event management (SIEM)

network protocol analyzer (packet sniffer)

operating system

programming language

Correct

Fill in the blank: A security team uses a \_\_\_\_\_ to help them document organizational processes from beginning to end. 1 / 1 point

legend

playbook

graph

toolkit

Correct

Question 5

As a security analyst, you are tasked with auditing your organization's network to identify security related issues. How might a network protocol analyzer (packet sniffer) help you perform this task? 1 / 1 point

By capturing and analyzing data traffic on the network

By automating tasks that reduce human error

By simulating attacks on connected devices

By removing malware and viruses from the network

Correct

Question 6

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

Complete repetitive tasks with a high degree of efficiency

Correct

Execute repetitive processes very accurately

Correct

Can be used to create a specific set of instructions for a computer to execute tasks

Correct

To provide details about any operational action

Question 7

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

command line

dashboard

ciphertext

error log

Correct

Question 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)

playbooks

logs

Correct

Question 9

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

It makes static data more dynamic.

It helps security professionals be more accurate.

Correct

It is designed for high levels of accuracy.

Correct

It simplifies repetitive tasks.

Correct