

Question 1

What tool is designed to capture and analyze data traffic within a network? 1 / 1 point
security information and event management (SIEM)

network protocol analyzer (packet sniffer)

playbook

Structured Query Language (SQL)

Correct

A packet sniffer, also known as a network protocol analyzer, is a tool designed to capture and analyze data traffic within a network.

Question 2

What type of tool uses dashboards to organize data into categories and allows analysts to identify potential security incidents as they happen? 1 / 1 point

Python

SIEM

network protocol analyzers (packet sniffers)

Linux

Correct

SIEM tools use dashboards to organize data into categories and allow analysts to identify potential security incidents, such breaches, as they happen.

Question 3

What can cybersecurity professionals use logs for? 1 / 1 point

To analyze data traffic within a network

To identify vulnerabilities and potential security breaches

To select which security team members will respond to an incident

To research and optimize processing capabilities within a network

Correct

Cybersecurity professionals can use logs to identify vulnerabilities and potential security breaches, as well as other potential security incidents.

Question 4

Fill in the blank: A _____ is a manual that provides details about operational actions. 1 / 1 point

case history

playbook

checklist

directory

Correct

A playbook is a manual that provides details about operational actions. Playbooks provide guidance when handling a security incident before, during, and after it has occurred.