Question 1

What is the primary purpose of logs during incident investigation? 1 / 1 point

To provide a record of event details

To manage alert volumes

To identify and diagnose system issues

To improve user experience

Correct

The primary purpose of logs during incident investigation is to provide a record of event details. Knowing what occurred on systems, networks, and devices helps security analysts identify unusual or malicious activity.

Question 2

A security analyst wants to determine whether a suspicious login was successful. Which log type would be most useful for this purpose? 1 / 1 point

Authentication

Firewall

System

Network

Correct

An authentication log would be most useful for this purpose. Authentication logs record login attempts, including whether a login was successful.

Question 3

In the following log, what action does the log entry record?

[ALLOW: wikipedia.org] Source: 192.167.1.1 Friday, 10 June 2022 11:36:12 1 / 1 point

Source

192.167.1.1

ALLOW

Friday, 10 June 2022 11:36:12

Correct

ALLOW refers to the action that has been recorded. In this instance, it allows access to wikipedia.org.

Question 4

Fill in the blank: ______ is the process of examining logs to identify events of interest. 1 / 1 point

Logging

Log analysis

Log forwarder

Log file

Correct

Log analysis is the process of examining logs to identify events of interest.