1. Question 1

What details do logs contain? Select all that apply. 1 / 1 point

Location

Correct

Time

Correct

Date

Correct

Forwarder

Question 2

What is the difference between a log and log analysis? 1 / 1 point

A log contains log file details. Log analysis involves the collection and storage of logs.

A log and log analysis both contain details of events, but they record details from different sources.

A log is a record of events that occur within an organization's systems. Log analysis is the process of examining logs to identify events of interest.

A log records details in log files. Log analysis involves a high-level overview of all events that happen on the network.

Correct

Question 3

Examine the following log:

```
<111>1 2020-04-12T23:20:50.52Z my.machine.com evntslog - ID01 [user@98274 iut="2"
eventSource="Mobile" eventID="24"][Priority@98274 class="low"] Computer A
```

What field value indicates the type of device that this event originated from? 1 / 1 point

my.machine.com

low

Mobile

Computer A

Correct

Question 4

What is the difference between a network-based intrusion detection system (NIDS) and a host-based intrusion detection system (HIDS)? 1 / 1 point

A NIDS monitors the activity of the host on which it is installed. A HIDS uses signature analysis to analyze network activity.

A NIDS logs and generates alerts. A HIDS system monitors endpoint activity.

Both NIDS and HIDS monitor systems and generate alerts, but a NIDS use agents.

A NIDS collects and monitors network traffic and network data. A HIDS monitors the activity of the host on which it is installed.

Correct

Question 5
Which rule option is used to indicate the number of times a signature is updated? 1 / 1 point
tcp
msg
rev
sid
Correct

Question 6
Which rule option is used to match based on the direction of network traffic? 1 / 1 point
message
content
sid
flow
Correct

Question 7
Fill in the blank: Suricata uses the _____ format for event and alert output. 1 / 1 point
EVE JSON
HTTP
HTML
CEF
Correct

Question 8
Fill in the blank: The asterisk symbol is also known as a(n) _____. 1 / 1 point
wildcard
label
Boolean operator
option
Correct

Question 9
Fill in the blank: Chronicle uses ______ to define detection rules. 1 / 1 point
UDM
SQL
YARA-L
SPL
Correct

Question 10

What are the steps in the SIEM process for data collection? Select three answers. 1 / 1 point

Collect

Correct

Unify

Normalize

Correct

Index

Correct