1. Which of the following refers to a record of events that occur within an organization's systems? **1 / 1 point**

- ○ Log forwarder
- ○ Log sources
- ◉ Logs
- ○ Occurrences

✓ **Correct**

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

- ◉ 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 and log analysis both contain details of events, but they record details from different sources.
- ○ A log contains log file details. Log analysis involves the collection and storage of logs.
- ○ A log records details in log files. Log analysis involves a high-level overview of all events that happen on the network.

✓ **Correct**

3. Examine the following log: **1 / 1 point**

```
<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?

- ○ `my.machine.com`
- ○ `Computer A`
- ◉ `Mobile`
- ○ `low`

✓ **Correct**

4. Fill in the blank: _____ analysis is a detection method used to find events of interest using patterns. **1 / 1 point**

- ○ Network
- ◉ Signature
- ○ Host
- ○ Endpoint

✓ **Correct**

5. Which rule option is used to indicate the number of times a signature is updated? **1 / 1 point**

- ○ `sid`
- ◉ `rev`
- ○ `msg`
- ○ `tcp`

✓ **Correct**

6. Which symbol is used to indicate a comment and is ignored in a Suricata signature file? **1 / 1 point**

- ◉ `#`
- ○ `>`
- ○ `:`
- ○ `$`

✓ **Correct**

7. Which type of log data does Suricata generate? Select all that apply. **1 / 1 point**

- [ ] Signature
- [x] Alert

Correct

- [x] Network telemetry

Correct

- [ ] Protocol

8. Which querying language does Splunk use? **1 / 1 point**

- ◉ Search Processing Language
- ○ Structured Querying Language
- ○ SIEM Processing Language
- ○ Structured Processing Language

Correct

9. Which Unified Data Model (UDM) field search specifies a security action? **1 / 1 point**

- ◉ `security_result.action`
- ○ `metadata.event_type`
- ○ `action`
- ○ `block`

Correct

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

- [ ] Unify
- [x] Index

Correct

- [x] Collect

Correct

- [x] Normalize

Correct