Congratulations! You passed!

Grade received 100%
Weekly challenge 4
Latest Submission Grade 100%
To pass 80% or higher
Quiz • 50 min

Go to next item

Review Learning Objectives

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

- Log forwarder
- Occurrences
- Log sources
- Logs

Correct

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

```
LoginEvent[2021/10/13 10:32:08.958711] auth_session_authenticator.cc:304 Regular user login 1
```

Which type of log is this?

- Network
- Authentication
- Application
- Location

Correct

3. Fill in the blank: A syslog entry contains a header, _____, and a message. **1 / 1 point**

- object
- structured-data
- eXtensible Markup Language
- tag

Correct

4. Consider the following scenario: **1 / 1 point**

A security analyst at a midsized company is tasked with installing and configuring a host-based intrusion detection system (HIDS) on a laptop. The security analyst installs the HIDS and wants to test whether it is working properly by simulating malicious activity. The security analyst runs unauthorized programs on the laptop, which the HIDS successfully detects and alerts on.

What is the laptop an example of?

- An agent
- An endpoint
- A signature
- A log forwarder

Correct

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

- `sid`
- `rev`
- `tcp`
- `msg`

Correct

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

- `$`
- `#`
- `:`
- `>`

Correct

7. Fill in the blank: Suricata uses the _____ format for event and alert output. **1 / 1 point**

- HTML
- HTTP
- EVE JSON
- CEF

Correct

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

- SIEM Processing Language
- Search Processing Language
- Structured Querying Language
- Structured Processing Language

Correct

9. What is the default method of search in Chronicle? **1 / 1 point**

- Non-normalized
- UDM
- YARA-L
- Raw log

Correct

10. Which step in the SIEM process involves the processing of raw data into a standardized and structured format? **1 / 1 point**

- Normalize
- Collect
- Index
- Process

Correct