03: Assisted Lab: Reviewing IoC and Threat Intelligence Sources

CySA+ (Exam CS0-003)

Congratulations, you passed!

Duration: 39 minutes, 55 seconds

☑ On the selected AlienVault Pulse page related to Mirai, what is one of the types of indicators? *Score: 1*

- ○ Host system
- ○ Victim ID
- ◉ FileHash
- ○ Registrar

Congratulations, you have answered the question correctly.

☑ Which of the following is not an option in the list of Filters for exploits on The Exploit Database? *Score: 1*

- ○ Authentication Bypass / Credentials Bypass
- ○ Code Injection
- ○ Deserialization
- ◉ Evil Twin / Rogue Access Point
- ○ Heap Overflow

Congratulations, you have answered the question correctly.

☑ Which of the following is not one of the eight headings in the Web Application Security Policy template? (Select all that apply) *Score: 1*

- ☑ Summary
- ☐ Overview
- ☐ Purpose
- ☐ Policy Compliance
- ☑ References
- ☐ Scope
- ☐ Revision History
- ☐ Definitions and Terms
- ☐ Policy
- ☐ Related Standards, Policies, and Processes
- ☑ Supplemental and Supporting Material

Congratulations, you have answered the question correctly.

☑ **confirm if c:\Users\jaime\Documents\Web_App_Security_Policy_v.1.1.docx exists and is not empty** *Score: 1*

Select the **Score** button to validate this task:

```
File c:\Users\jaime\Documents\Web_App_Security_Policy_v.1.1.docx exists and is not empty

Task complete
```

☑ CIS has a benchmark document for which of the following products? (Select all that apply) *Score: 1*

- ☑ Firefox
- ☑ Amazon Web Services
- ☐ Discord
- ☑ Apple MacOS
- ☑ Docker

Congratulations, you have answered the question correctly.

☑ What is the goal of researching and understanding IoCs? *Score: 1*

- ○ Improving response efficiency
- ○ Reducing resolution costs
- ◉ Detecting attempted and successful violations
- ○ Improving ROSI of IAM

Congratulations, you have answered the question correctly.

☑ What types of entities provide threat intelligence feeds? (Select all that apply) *Score: 1*

- ☑ Government agencies
- ☑ Commercial organizations
- ☐ Dark web groups
- ☑ Open-source community groups

Congratulations, you have answered the question correctly.

☑ What indicators are used to locate IoC entries on the AlienVault site? (Select all that apply) *Score: 1*

- ☑ Domain
- ☐ MAC
- ☑ URL
- ☑ IPv4 or IPv6
- ☑ Hostname
- ☐ OS type
- ☑ FileHash

Congratulations, you have answered the question correctly.

☑ What is unique about Exploit Database compared to most other exploit information sites and services? *Score: 1*

- ○ Indication of the types of targets
- ◉ Access to the source code of exploits
- ○ List new and zero-day exploits
- ○ Inclusion of exploits for hardware

Congratulations, you have answered the question correctly.

☑ What is a Google dork? *Score: 1*

- ○ A person who does not understand how to use keywords to search for content on Google
- ○ A listing of symbols used to alter search functions when used in Google searches
- ○ A type of hacker to performs OSINT using only Google searches
- ◉ A search expression which may use advanced operators to discover security issues of indexed websites through a Google search

Congratulations, you have answered the question correctly.