

312-85^{Q&As}

Certified Threat Intelligence Analyst

Pass EC-COUNCIL 312-85 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/312-85.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

Jim works as a security analyst in a large multinational company. Recently, a group of hackers penetrated into their organizational network and used a data staging technique to collect sensitive data. They collected all sorts of sensitive data about the employees and customers, business tactics of the organization, financial information, network infrastructure information and so on.

What should Jim do to detect the data staging before the hackers exfiltrate from the network?

- A. Jim should identify the attack at an initial stage by checking the content of the user agent field.
- B. Jim should analyze malicious DNS requests, DNS payload, unspecified domains, and destination of DNS requests.
- C. Jim should monitor network traffic for malicious file transfers, file integrity monitoring, and event logs.
- D. Jim should identify the web shell running in the network by analyzing server access, error logs, suspicious strings indicating encoding, user agent strings, and so on.

Correct Answer: C

QUESTION 2

An analyst is conducting threat intelligence analysis in a client organization, and during the information gathering process, he gathered information from the publicly available sources and analyzed to obtain a rich useful form of intelligence. The information source that he used is primarily used for national security, law enforcement, and for collecting intelligence required for business or strategic decision making.

Which of the following sources of intelligence did the analyst use to collect information?

- A. OPSEC
- B. ISAC
- C. OSINT
- D. SIGINT

Correct Answer: C

QUESTION 3

What is the correct sequence of steps involved in scheduling a threat intelligence program?

1.
Review the project charter
2.
Identify all deliverables

3.

Identify the sequence of activities

4.

Identify task dependencies

5.

Develop the final schedule

6.

Estimate duration of each activity

7.

Identify and estimate resources for all activities

8.

Define all activities

9.

Build a work breakdown structure (WBS)

A. 1-->9-->2-->8-->3-->7-->4-->6-->5

B. 3-->4-->5-->2-->1-->9-->8-->7-->6

C. 1-->2-->3-->4-->5-->6-->9-->8-->7

D. 1-->2-->3-->4-->5-->6-->7-->8-->9

Correct Answer: A

QUESTION 4

Michael, a threat analyst, works in an organization named TechTop, was asked to conduct a cyber-threat intelligence analysis. After obtaining information regarding threats, he has started analyzing the information and understanding the nature of the threats.

What stage of the cyber-threat intelligence is Michael currently in?

A. Unknown unknowns

B. Unknowns unknown

C. Known unknowns

D. Known knowns

Correct Answer: C

QUESTION 5

SecurityTech Inc. is developing a TI plan where it can drive more advantages in less funds. In the process of selecting a TI platform, it wants to incorporate a feature that ranks elements such as intelligence sources, threat actors, attacks, and digital assets of the organization, so that it can put in more funds toward the resources which are critical for the organization's security.

Which of the following key features should SecurityTech Inc. consider in their TI plan for selecting the TI platform?

- A. Search
- B. Open
- C. Workflow
- D. Scoring

Correct Answer: D

[Latest 312-85 Dumps](#)

[312-85 Study Guide](#)

[312-85 Exam Questions](#)