312-85Q&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

QUESTION 1

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

QUESTION 2

A threat analyst obtains an intelligence related to a threat, where the data is sent in the form of a connection request from a remote host to the server. From this data, he obtains only the IP address of the source and destination but no contextual information. While processing this data, he obtains contextual information stating that multiple connection requests from different geo-locations are received by the server within a short time span, and as a result, the server is stressed and gradually its performance has reduced. He further performed analysis on the information based on the past and present experience and concludes the attack experienced by the client organization.

Which of the following attacks is performed on the client organization?

A. DHCP attacks

B. MAC spoofing attack

C. Distributed Denial-of-Service (DDoS) attack

D. Bandwidth attack

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

Which of the following components refers to a node in the network that routes the traffic from a workstation to external command and control server and helps in identification of installed malware in the network?

A. Repeater

B. Gateway

C. Hub

D. Network interface card (NIC)

Correct Answer: B