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.passapply.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

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

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 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

Walter and Sons Company has faced major cyber attacks and lost confidential data. The company has decided to concentrate more on the security rather than other resources. Therefore, they hired Alice, a threat analyst, to perform data analysis. Alice was asked to perform qualitative data analysis to extract useful information from collected bulk data.

Which of the following techniques will help Alice to perform qualitative data analysis?

A. Regression analysis, variance analysis, and so on

B. Numerical calculations, statistical modeling, measurement, research, and so on.

C. Brainstorming, interviewing, SWOT analysis, Delphi technique, and so on

D. Finding links between data and discover threat-related information

Correct Answer: C

QUESTION 5

Mr. Bob, a threat analyst, is performing analysis of competing hypotheses (ACH). He has reached to a stage where he is required to apply his analysis skills effectively to reject as many hypotheses and select the best hypotheses from the identified bunch of hypotheses, and this is done with the help of listed evidence. Then, he prepares a matrix where all the screened hypotheses are placed on the top, and the listed evidence for the hypotheses are placed at the bottom.

What stage of ACH is Bob currently in?

A. Diagnostics

B. Evidence

C. Inconsistency

D. Refinement

Correct Answer: A