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.pass4itsure.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

A network administrator working in an ABC organization collected log files generated by a traffic monitoring system, which may not seem to have useful information, but after performing proper analysis by him, the same information can be used to detect an attack in the network.

Which of the following categories of threat information has he collected?

A. Advisories

B. Strategic reports

C. Detection indicators

D. Low-level data

Correct Answer: C

QUESTION 2

Tim is working as an analyst in an ABC organization. His organization had been facing many challenges in converting the raw threat intelligence data into meaningful contextual information. After inspection, he found that it was due to noise obtained from misrepresentation of data from huge data collections. Hence, it is important to clean the data before performing data analysis using techniques such as data reduction. He needs to choose an appropriate threat intelligence framework that automatically performs data collection, filtering, and analysis for his organization.

Which of the following threat intelligence frameworks should he choose to perform such task?

A. HighCharts

B. SIGVERIF

C. Threat grid

D. TC complete

Correct Answer: D

QUESTION 3

An XYZ organization hired Mr. Andrews, a threat analyst. In order to identify the threats and mitigate the effect of such threats, Mr. Andrews was asked to perform threat modeling. During the process of threat modeling, he collected important information about the treat actor and characterized the analytic behavior of the adversary that includes technological details, goals, and motives that can be useful in building a strong countermeasure.

What stage of the threat modeling is Mr. Andrews currently in?

A. System modeling

B. Threat determination and identification

C. Threat profiling and attribution

D. Threat ranking

Correct Answer: C

QUESTION 4

Lizzy, an analyst, wants to recognize the level of risks to the organization so as to plan countermeasures against cyber attacks. She used a threat modelling methodology where she performed the following stages: Stage 1: Build asset-based threat profiles Stage 2: Identify infrastructure vulnerabilities Stage 3: Develop security strategy and plans Which of the following threat modelling methodologies was used by Lizzy in the aforementioned scenario?

A. TRIKE

B. VAST

C. OCTAVE

D. DREAD

Correct Answer: C

QUESTION 5

ABC is a well-established cyber-security company in the United States. The organization implemented the automation of tasks such as data enrichment and indicator aggregation. They also joined various communities to increase their knowledge about the emerging threats. However, the security teams can only detect and prevent identified threats in a reactive approach.

Based on threat intelligence maturity model, identify the level of ABC to know the stage at which the organization stands with its security and vulnerabilities.

A. Level 2: increasing CTI capabilities

B. Level 3: CTI program in place

C. Level 1: preparing for CTI

D. Level 0: vague where to start

Correct Answer: A