

EC-Council

Exam Questions 312-85

Certified Threat Intelligence Analyst



NEW QUESTION 1

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

Answer: D

NEW QUESTION 2

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

Answer: C

NEW QUESTION 3

Steve works as an analyst in a UK-based firm. He was asked to perform network monitoring to find any evidence of compromise. During the network monitoring, he came to know that there are multiple logins from different locations in a short time span. Moreover, he also observed certain irregular log in patterns from locations where the organization does not have business relations. This resembles that somebody is trying to steal confidential information.

Which of the following key indicators of compromise does this scenario present?

- A. Unusual outbound network traffic
- B. Unexpected patching of systems
- C. Unusual activity through privileged user account
- D. Geographical anomalies

Answer: C

NEW QUESTION 4

Daniel is a professional hacker whose aim is to attack a system to steal data and money for profit. He performs hacking to obtain confidential data such as social security numbers, personally identifiable information (PII) of an employee, and credit card information. After obtaining confidential data, he further sells the information on the black market to make money.

Daniel comes under which of the following types of threat actor.

- A. Industrial spies
- B. State-sponsored hackers
- C. Insider threat
- D. Organized hackers

Answer: D

NEW QUESTION 5

Joe works as a threat intelligence analyst with Xsecurity Inc. He is assessing the TI program by comparing the project results with the original objectives by reviewing project charter. He is also reviewing the list of expected deliverables to ensure that each of those is delivered to an acceptable level of quality.

Identify the activity that Joe is performing to assess a TI program's success or failure.

- A. Determining the fulfillment of stakeholders
- B. Identifying areas of further improvement
- C. Determining the costs and benefits associated with the program
- D. Conducting a gap analysis

Answer: D

NEW QUESTION 6

Karry, a threat analyst at an XYZ organization, is performing threat intelligence analysis. During the data collection phase, he used a data collection method that involves no participants and is purely based on analysis and observation of activities and processes going on within the local boundaries of the organization.

Identify the type data collection method used by the Karry.

- A. Active data collection
- B. Passive data collection
- C. Exploited data collection
- D. Raw data collection

Answer: B

NEW QUESTION 7

Kathy wants to ensure that she shares threat intelligence containing sensitive information with the appropriate audience. Hence, she used traffic light protocol (TLP).

Which TLP color would you signify that information should be shared only within a particular community?

- A. Red
- B. White
- C. Green
- D. Amber

Answer: D

NEW QUESTION 8

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

Answer: D

NEW QUESTION 9

In which of the following forms of bulk data collection are large amounts of data first collected from multiple sources in multiple formats and then processed to achieve threat intelligence?

- A. Structured form
- B. Hybrid form
- C. Production form
- D. Unstructured form

Answer: D

NEW QUESTION 10

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

Answer: A

NEW QUESTION 10

H&P, Inc. is a small-scale organization that has decided to outsource the network security monitoring due to lack of resources in the organization. They are looking for the options where they can directly incorporate threat intelligence into their existing network defense solutions.

Which of the following is the most cost-effective methods the organization can employ?

- A. Recruit the right talent
- B. Look for an individual within the organization
- C. Recruit data management solution provider
- D. Recruit managed security service providers (MSSP)

Answer: D

NEW QUESTION 15

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

312-85 Practice Exam Features:

- * 312-85 Questions and Answers Updated Frequently
- * 312-85 Practice Questions Verified by Expert Senior Certified Staff
- * 312-85 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 312-85 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 312-85 Practice Test Here](#)