

EC-Council

Exam Questions 312-85

Certified Threat Intelligence Analyst



NEW QUESTION 1

Andrews and Sons Corp. has decided to share threat information among sharing partners. Garry, a threat analyst, working in Andrews and Sons Corp., has asked to follow a trust model necessary to establish trust between sharing partners. In the trust model used by him, the first organization makes use of a body of evidence in a second organization, and the level of trust between two organizations depends on the degree and quality of evidence provided by the first organization.

Which of the following types of trust model is used by Garry to establish the trust?

- A. Mediated trust
- B. Mandated trust
- C. Direct historical trust
- D. Validated trust

Answer: D

NEW QUESTION 2

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)

Answer: B

NEW QUESTION 3

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 4

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

Answer: A

NEW QUESTION 5

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 6

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 7

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 8

In a team of threat analysts, two individuals were competing over projecting their own hypotheses on a given malware. However, to find logical proofs to confirm their hypotheses, the threat intelligence manager used a de-biasing strategy that involves learning strategic decision making in the circumstances comprising multistep interactions with numerous representatives, either having or without any perfect relevant information. Which of the following de-biasing strategies the threat intelligence manager used to confirm their hypotheses?

- A. Game theory
- B. Machine learning
- C. Decision theory
- D. Cognitive psychology

Answer: C

NEW QUESTION 9

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

Answer: C

NEW QUESTION 10

Jian is a member of the security team at Trinity, Inc. He was conducting a real-time assessment of system activities in order to acquire threat intelligence feeds. He acquired feeds from sources like honeynets, P2P monitoring, infrastructure, and application logs. Which of the following categories of threat intelligence feed was acquired by Jian?

- A. Internal intelligence feeds
- B. External intelligence feeds
- C. CSV data feeds
- D. Proactive surveillance feeds

Answer: A

NEW QUESTION 10

Henry, a threat intelligence analyst at ABC Inc., is working on a threat intelligence program. He was assigned to work on establishing criteria for prioritization of intelligence needs and requirements.

Which of the following considerations must be employed by Henry to prioritize intelligence requirements?

- A. Understand frequency and impact of a threat
- B. Understand data reliability
- C. Develop a collection plan
- D. Produce actionable data

Answer: A

NEW QUESTION 13

.....

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](#)