

## Exam Questions 312-85

Certified Threat Intelligence Analyst

<https://www.2passeasy.com/dumps/312-85/>



#### NEW QUESTION 1

Enrage Tech Company hired Enrique, a security analyst, for performing threat intelligence analysis. While performing data collection process, he used a counterintelligence mechanism where a recursive DNS server is employed to perform interserver DNS communication and when a request is generated from any name server to the recursive DNS server, the recursive DNS servers log the responses that are received. Then it replicates the logged data and stores the data in the central database. Using these logs, he analyzed the malicious attempts that took place over DNS infrastructure.

Which of the following cyber counterintelligence (CCI) gathering technique has Enrique used for data collection?

- A. Data collection through passive DNS monitoring
- B. Data collection through DNS interrogation
- C. Data collection through DNS zone transfer
- D. Data collection through dynamic DNS (DDNS)

**Answer: B**

#### NEW QUESTION 2

Sam works as an analyst in an organization named InfoTech Security. He was asked to collect information from various threat intelligence sources. In meeting the deadline, he forgot to verify the threat intelligence sources and used data from an open-source data provider, who offered it at a very low cost. Through it was beneficial at the initial stage but relying on such data providers can produce unreliable data and noise putting the organization network into risk.

What mistake Sam did that led to this situation?

- A. Sam used unreliable intelligence sources.
- B. Sam used data without context.
- C. Sam did not use the proper standardization formats for representing threat data.
- D. Sam did not use the proper technology to use or consume the information.

**Answer: D**

#### NEW QUESTION 3

Kim, an analyst, is looking for an intelligence-sharing platform to gather and share threat information from a variety of sources. He wants to use this information to develop security policies to enhance the overall security posture of his organization.

Which of the following sharing platforms should be used by Kim?

- A. Cuckoo sandbox
- B. OmniPeek
- C. PortDroid network analysis
- D. Blueliv threat exchange network

**Answer: D**

#### NEW QUESTION 4

John, a professional hacker, is trying to perform APT attack on the target organization network. He gains access to a single system of a target organization and tries to obtain administrative login credentials to gain further access to the systems in the network using various techniques.

What phase of the advanced persistent threat lifecycle is John currently in?

- A. Initial intrusion
- B. Search and exfiltration
- C. Expansion
- D. Persistence

**Answer: C**

#### 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

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

**Answer: C**

#### NEW QUESTION 7

Which of the following characteristics of APT refers to numerous attempts done by the attacker to gain entry to the target's network?

- A. Risk tolerance
- B. Timeliness
- C. Attack origination points
- D. Multiphased

**Answer: C**

#### NEW QUESTION 8

In which of the following storage architecture is the data stored in a localized system, server, or storage hardware and capable of storing a limited amount of data in its database and locally available for data usage?

- A. Distributed storage
- B. Object-based storage
- C. Centralized storage
- D. Cloud storage

**Answer: B**

#### NEW QUESTION 9

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 10

An organization suffered many major attacks and lost critical information, such as employee records, and financial information. Therefore, the management decides to hire a threat analyst to extract the strategic threat intelligence that provides high-level information regarding current cyber-security posture, threats, details on the financial impact of various cyber-activities, and so on.

Which of the following sources will help the analyst to collect the required intelligence?

- A. Active campaigns, attacks on other organizations, data feeds from external third parties
- B. OSINT, CTI vendors, ISAO/ISACs
- C. Campaign reports, malware, incident reports, attack group reports, human intelligence
- D. Human, social media, chat rooms

**Answer: B**

#### NEW QUESTION 10

Miley, an analyst, wants to reduce the amount of collected data and make the storing and sharing process easy. She uses filtering, tagging, and queuing technique to sort out the relevant and structured data from the large amounts of unstructured data.

Which of the following techniques was employed by Miley?

- A. Sandboxing
- B. Normalization
- C. Data visualization
- D. Convenience sampling

**Answer: B**

#### NEW QUESTION 12

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 15

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 18

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 22

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 24

Tyrion, a professional hacker, is targeting an organization to steal confidential information. He wants to perform website footprinting to obtain the following information, which is hidden in the web page header.

- Connection status and content type
- Accept-ranges and last-modified information
- X-powered-by information
- Web server in use and its version

Which of the following tools should the Tyrion use to view header content?

- A. Hydra
- B. AutoShun
- C. Vanguard enforcer
- D. Burp suite

**Answer: D**

#### NEW QUESTION 29

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 30

Moses, a threat intelligence analyst at InfoTec Inc., wants to find crucial information about the potential threats the organization is facing by using advanced Google search operators. He wants to identify whether any fake websites are hosted at the similar to the organization's URL.

Which of the following Google search queries should Moses use?

- A. related: www.infothech.org
- B. info: www.infothech.org
- C. link: www.infothech.org
- D. cache: www.infothech.org

**Answer: A**

#### NEW QUESTION 33

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 38

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-85 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-85 Product From:

<https://www.2passeasy.com/dumps/312-85/>

### Money Back Guarantee

#### **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 FirstTry
- \* 312-85 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year