

## Exam Questions 312-85

Certified Threat Intelligence Analyst

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



#### 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

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 4

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 5

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.

**Answer: C**

#### NEW QUESTION 6

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 7

Which of the following types of threat attribution deals with the identification of the specific person, society, or a country sponsoring a well-planned and executed intrusion or attack over its target?

- A. Nation-state attribution
- B. True attribution
- C. Campaign attribution
- D. Intrusion-set attribution

Answer: B

#### NEW QUESTION 8

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 9

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 threat 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 10

A team of threat intelligence analysts is performing threat analysis on malware, and each of them has come up with their own theory and evidence to support their theory on a given malware.

Now, to identify the most consistent theory out of all the theories, which of the following analytic processes must threat intelligence manager use?

- A. Threat modelling
- B. Application decomposition and analysis (ADA)
- C. Analysis of competing hypotheses (ACH)
- D. Automated technical analysis

Answer: C

#### NEW QUESTION 10

Bob, a threat analyst, works in an organization named TechTop. He was asked to collect intelligence to fulfil the needs and requirements of the Red Team present within the organization.

Which of the following are the needs of a RedTeam?

- A. Intelligence related to increased attacks targeting a particular software or operating system vulnerability
- B. Intelligence on latest vulnerabilities, threat actors, and their tactics, techniques, and procedures (TTPs)
- C. Intelligence extracted latest attacks analysis on similar organizations, which includes details about latest threats and TTPs
- D. Intelligence that reveals risks related to various strategic business decisions

Answer: B

#### NEW QUESTION 12

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 16**

Jame, a professional hacker, is trying to hack the confidential information of a target organization. He identified the vulnerabilities in the target system and created a tailored deliverable malicious payload using an exploit and a backdoor to send it to the victim.

Which of the following phases of cyber kill chain methodology is Jame executing?

- A. Reconnaissance
- B. Installation
- C. Weaponization
- D. Exploitation

**Answer: C**

**NEW QUESTION 21**

Alice, a threat intelligence analyst at HiTech Cyber Solutions, wants to gather information for identifying emerging threats to the organization and implement essential techniques to prevent their systems and networks from such attacks. Alice is searching for online sources to obtain information such as the method used to launch an attack, and techniques and tools used to perform an attack and the procedures followed for covering the tracks after an attack.

Which of the following online sources should Alice use to gather such information?

- A. Financial services
- B. Social network settings
- C. Hacking forums
- D. Job sites

**Answer: C**

**NEW QUESTION 23**

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 27**

.....

## 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