



## **EC-Council**

### **Exam Questions 312-85**

Certified Threat Intelligence Analyst

#### NEW QUESTION 1

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 2

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 3

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 4

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 5

Cybersol Technologies initiated a cyber-threat intelligence program with a team of threat intelligence analysts.

During the process, the analysts started converting the raw data into useful information by applying various techniques, such as machine-based techniques, and statistical methods.

In which of the following phases of the threat intelligence lifecycle is the threat intelligence team currently working?

- A. Dissemination and integration
- B. Planning and direction
- C. Processing and exploitation
- D. Analysis and production

**Answer: A**

#### NEW QUESTION 6

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 7

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 8

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 9

An analyst is conducting threat intelligence analysis in a client organization, and during the information gathering process, he gathered information from the publicly available sources and analyzed to obtain a rich useful form of intelligence. The information source that he used is primarily used for national security, law enforcement, and for collecting intelligence required for business or strategic decision making.

Which of the following sources of intelligence did the analyst use to collect information?

- A. OPSEC
- B. ISAC
- C. OSINT
- D. SIGINT

**Answer: C**

#### NEW QUESTION 10

Tracy works as a CISO in a large multinational company. She consumes threat intelligence to understand the changing trends of cyber security. She requires intelligence to understand the current business trends and make appropriate decisions regarding new technologies, security budget, improvement of processes, and staff. The intelligence helps her in minimizing business risks and protecting the new technology and business initiatives.

Identify the type of threat intelligence consumer is Tracy.

- A. Tactical users
- B. Strategic users
- C. Operational users
- D. Technical users

**Answer: B**

#### NEW QUESTION 10

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 15

A threat analyst obtains an intelligence related to a threat, where the data is sent in the form of a connection request from a remote host to the server. From this data, he obtains only the IP address of the source and destination but no contextual information. While processing this data, he obtains contextual information stating that multiple connection requests from different geo-locations are received by the server within a short time span, and as a result, the server is stressed and gradually its performance has reduced. He further performed analysis on the information based on the past and present experience and concludes the attack experienced by the client organization.

Which of the following attacks is performed on the client organization?

- A. DHCP attacks
- B. MAC spoofing attack
- C. Distributed Denial-of-Service (DDoS) attack
- D. Bandwidth attack

**Answer:** C

#### NEW QUESTION 17

Alison, an analyst in an XYZ organization, wants to retrieve information about a company's website from the time of its inception as well as the removed information from the target website.

What should Alison do to get the information he needs.

- A. Alison should use SmartWhois to extract the required website information.
- B. Alison should use <https://archive.org> to extract the required website information.
- C. Alison should run the Web Data Extractor tool to extract the required website information.
- D. Alison should recover cached pages of the website from the Google search engine cache to extract the required website information.

**Answer:** C

#### NEW QUESTION 20

Michael, a threat analyst, works in an organization named TechTop, was asked to conduct a cyber-threat intelligence analysis. After obtaining information regarding threats, he has started analyzing the information and understanding the nature of the threats.

What stage of the cyber-threat intelligence is Michael currently in?

- A. Unknown unknowns
- B. Unknowns unknown
- C. Known unknowns
- D. Known knowns

**Answer:** C

#### NEW QUESTION 24

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 27

Sarah is a security operations center (SOC) analyst working at JW Williams and Sons organization based in Chicago. As a part of security operations, she contacts information providers (sharing partners) for gathering information such as collections of validated and prioritized threat indicators along with a detailed technical analysis of malware samples, botnets, DDoS attack methods, and various other malicious tools. She further used the collected information at the tactical and operational levels.

Sarah obtained the required information from which of the following types of sharing partner?

- A. Providers of threat data feeds
- B. Providers of threat indicators
- C. Providers of comprehensive cyber-threat intelligence
- D. Providers of threat actors

**Answer:** C

#### NEW QUESTION 31

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 34

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questons 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 FirstTry
- \* 312-85 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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