



## **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

ABC is a well-established cyber-security company in the United States. The organization implemented the automation of tasks such as data enrichment and indicator aggregation. They also joined various communities to increase their knowledge about the emerging threats. However, the security teams can only detect and prevent identified threats in a reactive approach.

Based on threat intelligence maturity model, identify the level of ABC to know the stage at which the organization stands with its security and vulnerabilities.

- A. Level 2: increasing CTI capabilities
- B. Level 3: CTI program in place
- C. Level 1: preparing for CTI
- D. Level 0: vague where to start

**Answer:** A

#### NEW QUESTION 3

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 4

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 5

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 6

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 7

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 8

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 9

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 10

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 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 15

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 16

Alice, an analyst, shared information with security operation managers and network operations center (NOC) staff for protecting the organizational resources against various threats. Information shared by Alice was highly technical and include threat actor TTPs, malware campaigns, tools used by threat actors, and so on.

Which of the following types of threat intelligence was shared by Alice?

- A. Strategic threat intelligence
- B. Tactical threat intelligence
- C. Technical threat intelligence
- D. Operational threat intelligence

**Answer: C**

#### NEW QUESTION 19

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 24

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 28

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

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

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 36

.....

## 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](#)**