

# 312-85<sup>Q&As</sup>

Certified Threat Intelligence Analyst

## Pass EC-COUNCIL 312-85 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/312-85.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

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

Correct Answer: D

---

**QUESTION 2**

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

Correct Answer: D

---

**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

Correct Answer: A

---

#### QUESTION 4

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

Correct Answer: C

---

#### QUESTION 5

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)

Correct Answer: B

---

#### QUESTION 6

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

Correct Answer: B

---

#### QUESTION 7

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

Correct Answer: A

---

#### QUESTION 8

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.

Correct Answer: C

---

#### QUESTION 9

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

Correct Answer: D

---

#### QUESTION 10

During the process of threat intelligence analysis, John, a threat analyst, successfully extracted an indication of adversary's information, such as Modus operandi, tools, communication channels, and forensics evasion strategies used by adversaries.

Identify the type of threat intelligence analysis is performed by John.

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

Correct Answer: D

---

[Latest 312-85 Dumps](#)

[312-85 Practice Test](#)

[312-85 Study Guide](#)