



# 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.pass4itsure.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**

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

Correct Answer: C

---

**QUESTION 2**

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

Correct Answer: C

---

**QUESTION 3**

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



Correct Answer: C

---

#### QUESTION 4

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 5

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

[Latest 312-85 Dumps](#)

[312-85 Study Guide](#)

[312-85 Exam Questions](#)