



312-85^{Q&As}

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**

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 2

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

Correct Answer: C

QUESTION 3

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

Correct Answer: B

**QUESTION 4**

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

Correct Answer: C

QUESTION 5

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

Correct Answer: C

[Latest 312-85 Dumps](#)

[312-85 PDF Dumps](#)

[312-85 Study Guide](#)