



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**

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

Correct Answer: C

QUESTION 2

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

Correct Answer: A

QUESTION 3

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.

Correct Answer: C

QUESTION 4

Kathy wants to ensure that she shares threat intelligence containing sensitive information with the appropriate audience. Hence, she used traffic light protocol (TLP). Which TLP color would you signify that information should be shared only within a particular community?

- A. Red
- B. White
- C. Green
- D. Amber

Correct Answer: D

QUESTION 5

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

Correct Answer: B

[Latest 312-85 Dumps](#)

[312-85 Practice Test](#)

[312-85 Study Guide](#)