



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.geekcert.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

Steve works as an analyst in a UK-based firm. He was asked to perform network monitoring to find any evidence of compromise. During the network monitoring, he came to know that there are multiple logins from different locations in a short time span. Moreover, he also observed certain irregular log in patterns from locations where the organization does not have business relations. This resembles that somebody is trying to steal confidential information.

Which of the following key indicators of compromise does this scenario present?

- A. Unusual outbound network traffic
- B. Unexpected patching of systems
- C. Unusual activity through privileged user account
- D. Geographical anomalies

Correct Answer: C

QUESTION 2

HandP, 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)

Correct Answer: D

QUESTION 3

Mr. Bob, a threat analyst, is performing analysis of competing hypotheses (ACH). He has reached to a stage where he is required to apply his analysis skills effectively to reject as many hypotheses and select the best hypotheses from the identified bunch of hypotheses, and this is done with the help of listed evidence. Then, he prepares a matrix where all the screened hypotheses are placed on the top, and the listed evidence for the hypotheses are placed at the bottom.

What stage of ACH is Bob currently in?

- A. Diagnostics
- B. Evidence
- C. Inconsistency



D. Refinement

Correct Answer: A

QUESTION 4

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 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

[312-85 VCE Dumps](#)

[312-85 Study Guide](#)

[312-85 Braindumps](#)