



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.passapply.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

Walter and Sons Company has faced major cyber attacks and lost confidential data. The company has decided to concentrate more on the security rather than other resources. Therefore, they hired Alice, a threat analyst, to perform data analysis. Alice was asked to perform qualitative data analysis to extract useful information from collected bulk data.

Which of the following techniques will help Alice to perform qualitative data analysis?

- A. Regression analysis, variance analysis, and so on
- B. Numerical calculations, statistical modeling, measurement, research, and so on.
- C. Brainstorming, interviewing, SWOT analysis, Delphi technique, and so on
- D. Finding links between data and discover threat-related information

Correct Answer: C

QUESTION 2

A threat analyst obtains an intelligence related to a threat, where the data is sent in the form of a connection request from a remote host to the server. From this data, he obtains only the IP address of the source and destination but no contextual information. While processing this data, he obtains contextual information stating that multiple connection requests from different geo-locations are received by the server within a short time span, and as a result, the server is stressed and gradually its performance has reduced. He further performed analysis on the information based on the past and present experience and concludes the attack experienced by the client organization.

Which of the following attacks is performed on the client organization?

- A. DHCP attacks
- B. MAC spoofing attack
- C. Distributed Denial-of-Service (DDoS) attack
- D. Bandwidth attack

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

In which of the following storage architecture is the data stored in a localized system, server, or storage hardware and capable of storing a limited amount of data in its database and locally available for data usage?

- A. Distributed storage
- B. Object-based storage
- C. Centralized storage
- D. Cloud storage

Correct Answer: B

QUESTION 5

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 VCE Dumps](#)

[312-85 Braindumps](#)