312-85Q&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

Michael, a threat analyst, works in an organization named TechTop, was asked to conduct a cyber-threat intelligence analysis. After obtaining information regarding threats, he has started analyzing the information and understanding the nature of the threats.

What stage of the cyber-threat intelligence is Michael currently in?

A. Unknown unknowns

B. Unknowns unknown

C. Known unknowns

D. Known knowns

Correct Answer: C

QUESTION 2

Jim works as a security analyst in a large multinational company. Recently, a group of hackers penetrated into their organizational network and used a data staging technique to collect sensitive data. They collected all sorts of sensitive data about the employees and customers, business tactics of the organization, financial information, network infrastructure information and so on.

What should Jim do to detect the data staging before the hackers exfiltrate from the network?

A. Jim should identify the attack at an initial stage by checking the content of the user agent field.

B. Jim should analyze malicious DNS requests, DNS payload, unspecified domains, and destination of DNS requests.

C. Jim should monitor network traffic for malicious file transfers, file integrity monitoring, and event logs.

D. Jim should identify the web shell running in the network by analyzing server access, error logs, suspicious strings indicating encoding, user agent strings, and so on.

Correct Answer: C

QUESTION 3

Kim, an analyst, is looking for an intelligence-sharing platform to gather and share threat information from a variety of sources. He wants to use this information to develop security policies to enhance the overall security posture of his organization.

Which of the following sharing platforms should be used by Kim?

A. Cuckoo sandbox

B. OmniPeek

C. PortDroid network analysis

D. Blueliv threat exchange network

Correct Answer: D

QUESTION 4

In which of the following attacks does the attacker exploit vulnerabilities in a computer application before the software developer can release a patch for them?

A. Active online attack

B. Zero-day attack

C. Distributed network attack

D. Advanced persistent attack

Correct Answer: B

QUESTION 5

In which of the following forms of bulk data collection are large amounts of data first collected from multiple sources in multiple formats and then processed to achieve threat intelligence?

A. Structured form

B. Hybrid form

C. Production form

D. Unstructured form

Correct Answer: D