

DUMPSBOSS.COM

Certified Threat Intelligence Analyst

ECCouncil 312-85

Version Demo

Total Demo Questions: 10

Total Premium Questions: 49

Buy Premium PDF

<https://dumpsboss.com>

support@dumpsboss.com

dumpsboss.com

QUESTION NO: 1

Karry, a threat analyst at an XYZ organization, is performing threat intelligence analysis. During the data collection phase, he used a data collection method that involves no participants and is purely based on analysis and observation of activities and processes going on within the local boundaries of the organization.

Identify the type data collection method used by the Karry.

- A. Active data collection
- B. Passive data collection
- C. Exploited data collection
- D. Raw data collection

ANSWER: B**QUESTION NO: 2**

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

ANSWER: B**QUESTION NO: 3**

Which of the following characteristics of APT refers to numerous attempts done by the attacker to gain entry to the target's network?

- A. Risk tolerance
- B. Timeliness
- C. Attack origination points
- D. Multiphased

ANSWER: C**QUESTION NO: 4**

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.

ANSWER: C**QUESTION NO: 5**

Tim is working as an analyst in an ABC organization. His organization had been facing many challenges in converting the raw threat intelligence data into meaningful contextual information. After inspection, he found that it was due to noise obtained from misrepresentation of data from huge data collections. Hence, it is important to clean the data before performing data analysis using techniques such as data reduction. He needs to choose an appropriate threat intelligence framework that automatically performs data collection, filtering, and analysis for his organization.

Which of the following threat intelligence frameworks should he choose to perform such task?

- A. HighCharts
- B. SIGVERIF
- C. Threat grid
- D. TC complete

ANSWER: D**QUESTION NO: 6**

What is the correct sequence of steps involved in scheduling a threat intelligence program?

1. Review the project charter
2. Identify all deliverables

3. Identify the sequence of activities
 4. Identify task dependencies
 5. Develop the final schedule
 6. Estimate duration of each activity
 7. Identify and estimate resources for all activities
 8. Define all activities
 9. Build a work breakdown structure (WBS)
- A. 1-->9-->2-->8-->3-->7-->4-->6-->5
- B. 3-->4-->5-->2-->1-->9-->8-->7-->6
- C. 1-->2-->3-->4-->5-->6-->9-->8-->7
- D. 1-->2-->3-->4-->5-->6-->7-->8-->9

ANSWER: A

QUESTION NO: 7

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 threat 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

ANSWER: C

QUESTION NO: 8

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

ANSWER: B

QUESTION NO: 9

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.

ANSWER: C

QUESTION NO: 10

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

ANSWER: D