# 312-85 Dumps

# Certified Threat Intelligence Analyst

## https://www.certleader.com/312-85-dumps.html
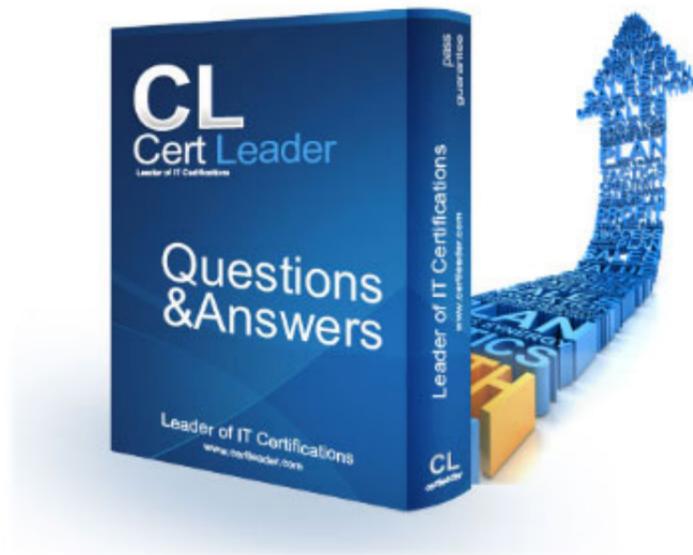
**NEW QUESTION 1**
Sam works as an analyst in an organization named InfoTech Security. He was asked to collect information from various threat intelligence sources. In meeting the deadline, he forgot to verify the threat intelligence sources and used data from an open-source data provider, who offered it at a very low cost. Through it was beneficial at the initial stage but relying on such data providers can produce unreliable data and noise putting the organization network into risk.
What mistake Sam did that led to this situation?

A. Sam used unreliable intelligence sources.
B. Sam used data without context.
C. Sam did not use the proper standardization formats for representing threat data.
D. Sam did not use the proper technology to use or consume the information.

**Answer:** D

**NEW QUESTION 2**
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

**Answer:** D

**NEW QUESTION 3**
John, a professional hacker, is trying to perform APT attack on the target organization network. He gains access to a single system of a target organization and tries to obtain administrative login credentials to gain further access to the systems in the network using various techniques.
What phase of the advanced persistent threat lifecycle is John currently in?

A. Initial intrusion
B. Search and exfiltration
C. Expansion
D. Persistence

**Answer:** C

**NEW QUESTION 4**
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

**Answer:** C

**NEW QUESTION 5**
Cybersol Technologies initiated a cyber-threat intelligence program with a team of threat intelligence analysts.
During the process, the analysts started converting the raw data into useful information by applying various techniques, such as machine-based techniques, and statistical methods.
In which of the following phases of the threat intelligence lifecycle is the threat intelligence team currently working?

A. Dissemination and integration
B. Planning and direction
C. Processing and exploitation
D. Analysis and production

**Answer:** A

**NEW QUESTION 6**
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

**Answer:** B

**NEW QUESTION 7**

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

**Answer:** D


**NEW QUESTION 8**
A network administrator working in an ABC organization collected log files generated by a traffic monitoring system, which may not seem to have useful information, but after performing proper analysis by him, the same information can be used to detect an attack in the network.
Which of the following categories of threat information has he collected?

A. Advisories
B. Strategic reports
C. Detection indicators
D. Low-level data

**Answer:** C


**NEW QUESTION 9**
Jame, a professional hacker, is trying to hack the confidential information of a target organization. He identified the vulnerabilities in the target system and created a tailored deliverable malicious payload using an exploit and a backdoor to send it to the victim.
Which of the following phases of cyber kill chain methodology is Jame executing?

A. Reconnaissance
B. Installation
C. Weaponization
D. Exploitation

**Answer:** C


**NEW QUESTION 10**
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

**Answer:** C


**NEW QUESTION 10**
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


**NEW QUESTION 13**
Sarah is a security operations center (SOC) analyst working at JW Williams and Sons organization based in Chicago. As a part of security operations, she contacts information providers (sharing partners) for gathering information such as collections of validated and prioritized threat indicators along with a detailed technical analysis of malware samples, botnets, DDoS attack methods, and various other malicious tools. She further used the collected information at the tactical and operational levels.
Sarah obtained the required information from which of the following types of sharing partner?

A. Providers of threat data feeds
B. Providers of threat indicators
C. Providers of comprehensive cyber-threat intelligence
D. Providers of threat actors

**Answer:** C


**NEW QUESTION 17**
Moses, a threat intelligence analyst at InfoTec Inc., wants to find crucial information about the potential threats the organization is facing by using advanced Google search operators. He wants to identify whether any fake websites are hosted at the similar to the organization's URL.

Which of the following Google search queries should Moses use?

A. related: www.infothech.org
B. info: www.infothech.org
C. link: www.infothech.org
D. cache: www.infothech.org

**Answer:** A


**NEW QUESTION 20**
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

**Answer:** A


**NEW QUESTION 22**
An attacker instructs bots to use camouflage mechanism to hide his phishing and malware delivery locations in the rapidly changing network of compromised bots. In this particular technique, a single domain name consists of multiple IP addresses.
Which of the following technique is used by the attacker?

A. DNS zone transfer
B. Dynamic DNS
C. DNS interrogation
D. Fast-Flux DNS

**Answer:** D


**NEW QUESTION 25**
......

# Thank You for Trying Our Product

* 100% Pass or Money Back

  All our products come with a 90-day Money Back Guarantee.

* One year free update

  You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

  We currently serve more than 30,000,000 customers.

* Shop Securely

  All transactions are protected by VeriSign!

**100% Pass Your 312-85 Exam with Our Prep Materials Via below:**

https://www.certleader.com/312-85-dumps.html