Vendor:EC-COUNCIL

Exam Code:312-85

Exam Name: Certified Threat Intelligence Analyst

Version: Demo

QUESTION 1

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

QUESTION 2

Henry. a threat intelligence analyst at ABC Inc., is working on a threat intelligence program. He was assigned to work on establishing criteria for prioritization of intelligence needs and requirements. Which of the following considerations must be employed by Henry to prioritize intelligence requirements?

A. Understand frequency and impact of a threat

B. Understand data reliability

C. Develop a collection plan

D. Produce actionable data

Correct Answer: A

QUESTION 3

Bob, a threat analyst, works in an organization named TechTop. He was asked to collect intelligence to fulfil the needs and requirements of the Red Tam present within the organization. Which of the following are the needs of a RedTeam?

A. Intelligence related to increased attacks targeting a particular software or operating system vulnerability

B. Intelligence on latest vulnerabilities, threat actors, and their tactics, techniques, and procedures (TTPs)

C. Intelligence extracted latest attacks analysis on similar organizations, which includes details about latest threats and TTPs

D. Intelligence that reveals risks related to various strategic business decisions

Correct Answer: B

QUESTION 4

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

Correct Answer: A

QUESTION 5

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 6

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.

Correct Answer: D

QUESTION 7

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 8

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

Correct Answer: D

QUESTION 9

ABC is a well-established cyber-security company in the United States. The organization implemented the automation of tasks such as data enrichment and indicator aggregation. They also joined various communities to increase their knowledge about the emerging threats. However, the security teams can only detect and prevent identified threats in a reactive approach.

Based on threat intelligence maturity model, identify the level of ABC to know the stage at which the organization stands with its security and vulnerabilities.

A. Level 2: increasing CTI capabilities

B. Level 3: CTI program in place

C. Level 1: preparing for CTI

D. Level 0: vague where to start

Correct Answer: A

QUESTION 10

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

Correct Answer: A

QUESTION 11

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

Correct Answer: C

QUESTION 12

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.

Correct Answer: C