312-85 Tested & Approved Certified Threat Intelligence Analyst Study Materials [Q23-Q41

312-85 Tested & Approved Certified Threat Intelligence Analyst Study Materials
Validate your Skills with Updated Certified Threat Intelligence Analyst Exam Questions & Answers and Test Engine
QUESTION 23

Alice, a threat intelligence analyst at HiTech Cyber Solutions, wants to gather information for identifying emerging threats to the organization and implement essential techniques to prevent their systems and networks from such attacks. Alice is searching for online sources to obtain information such as the method used to launch an attack, and techniques and tools used to perform an attack and the procedures followed for covering the tracks after an attack.

Which of the following online sources should Alice use to gather such information?
* Financial services
* Social network settings
* Hacking forums
* Job sites

QUESTION 24

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?
* Structured form
* Hybrid form
* Production form
* Unstructured form

QUESTION 25

Tyrion, a professional hacker, is targeting an organization to steal confidential information. He wants to perform website footprinting to obtain the following information, which is hidden in the web page header.

Connection status and content type

Accept-ranges and last-modified information

X-powered-by information

Web server in use and its version

Which of the following tools should the Tyrion use to view header content?
* Hydra
* AutoShun
* Vanguard enforcer
* Burp suite

QUESTION 26

Enrage Tech Company hired Enrique, a security analyst, for performing threat intelligence analysis. While performing data collection process, he used a counterintelligence mechanism where a recursive DNS server is employed to perform interserver DNS communication and when a request is generated from any name server to the recursive DNS server, the recursive DNS servers log the responses that are received. Then it replicates the logged data and stores the data in the central database. Using these logs, he analyzed the malicious attempts that took place over DNS infrastructure.

Which of the following cyber counterintelligence (CCI) gathering technique has Enrique used for data collection?
* Data collection through passive DNS monitoring
* Data collection through DNS interrogation
* Data collection through DNS zone transfer
* Data collection through dynamic DNS (DDNS)

QUESTION 27

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?
* Dissemination and integration
* Planning and direction
* Processing and exploitation

* Analysis and production

QUESTION 28

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 dat a. 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?
* Jim should identify the attack at an initial stage by checking the content of the user agent field.
* Jim should analyze malicious DNS requests, DNS payload, unspecified domains, and destination of DNS requests.
* Jim should monitor network traffic for malicious file transfers, file integrity monitoring, and event logs.
* 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.

QUESTION 29

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?
* Initial intrusion
* Search and exfiltration
* Expansion
* Persistence

QUESTION 30

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?
* Understand frequency and impact of a threat
* Understand data reliability
* Develop a collection plan
* Produce actionable data

QUESTION 31

An analyst is conducting threat intelligence analysis in a client organization, and during the information gathering process, he gathered information from the publicly available sources and analyzed to obtain a rich useful form of intelligence. The information source that he used is primarily used for national security, law enforcement, and for collecting intelligence required for business or strategic decision making.

Which of the following sources of intelligence did the analyst use to collect information?
* OPSEC
* ISAC
* OSINT
* SIGINT

QUESTION 32

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?
* Distributed storage
* Object-based storage
* Centralized storage
* Cloud storage

QUESTION 33

Andrews and Sons Corp. has decided to share threat information among sharing partners. Garry, a threat analyst, working in Andrews and Sons Corp., has asked to follow a trust model necessary to establish trust between sharing partners. In the trust model used by him, the first organization makes use of a body of evidence in a second organization, and the level of trust between two organizations depends on the degree and quality of evidence provided by the first organization.

Which of the following types of trust model is used by Garry to establish the trust?
* Mediated trust
* Mandated trust
* Direct historical trust
* Validated trust

QUESTION 34

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?
* Internal intelligence feeds
* External intelligence feeds
* CSV data feeds
* Proactive surveillance feeds

QUESTION 35

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?
* Red
* White
* Green
* Amber

QUESTION 36

An analyst wants to disseminate the information effectively so that the consumers can acquire and benefit out of the intelligence.

Which of the following criteria must an analyst consider in order to make the intelligence concise, to the point, accurate, and easily understandable and must consist of a right balance between tables, narrative, numbers, graphics, and multimedia?
* The right time
* The right presentation
* The right order
* The right content

QUESTION 37

An organization suffered many major attacks and lost critical information, such as employee records, and financial information. Therefore, the management decides to hire a threat analyst to extract the strategic threat intelligence that provides high-level information regarding current cyber-security posture, threats, details on the financial impact of various cyber-activities, and so on.

Which of the following sources will help the analyst to collect the required intelligence?
* Active campaigns, attacks on other organizations, data feeds from external third parties
* OSINT, CTI vendors, ISAO/ISACs
* Campaign reports, malware, incident reports, attack group reports, human intelligence
* Human, social media, chat rooms

QUESTION 38

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?
* Sandboxing
* Normalization
* Data visualization
* Convenience sampling

QUESTION 39

SecurityTech Inc. is developing a TI plan where it can drive more advantages in less funds. In the process of selecting a TI platform, it wants to incorporate a feature that ranks elements such as intelligence sources, threat actors, attacks, and digital assets of the organization, so that it can put in more funds toward the resources which are critical for the organization’s security.

Which of the following key features should SecurityTech Inc. consider in their TI plan for selecting the TI platform?
* Search
* Open
* Workflow
* Scoring

QUESTION 40

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?
* related: www.infothech.org

* info: www.infothech.org
* link: www.infothech.org
* cache: www.infothech.org

QUESTION 41

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?
* Intelligence related to increased attacks targeting a particular software or operating system vulnerability
* Intelligence on latest vulnerabilities, threat actors, and their tactics, techniques, and procedures (TTPs)
* Intelligence extracted latest attacks analysis on similar organizations, which includes details about latest threats and TTPs
* Intelligence that reveals risks related to various strategic business decisions

ECCouncil 312-85 Exam Syllabus Topics:

TopicDetailsTopic 1- Understanding Organization's Current Threat Landscape- Reviewing Threat Intelligence ProgramTopic 2- Overview of Fine-Tuning Threat Analysis- Understanding Threat Intelligence EvaluationTopic 3- Overview of Threat Intelligence Integration- Overview of Threat Intelligence ReportsTopic 4- Understanding Threat Intelligence Data Collection and Acquisition- Overview of Threat Intelligence Collection ManagementTopic 5- Overview of Threat Intelligence Lifecycle and Frameworks- Introduction to Threat IntelligenceTopic 6- Cyber Threats and Kill Chain Methodology- Understanding Cyber Kill ChainTopic 7- Understanding Indicators of Compromise- Understanding Advanced Persistent ThreatsTopic 8- Overview of Threat Intelligence Sharing- Requirements, Planning, Direction, and ReviewTopic 9- Understanding Cyber Threat Intelligence- Understanding IntelligenceTopic 10- Understanding Requirements Analysis- Building a Threat Intelligence Team