EC-Council

Exam Questions 312-85

Certified Threat Intelligence Analyst

NEW QUESTION 1
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

Answer: A

NEW QUESTION 2
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 3
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

NEW QUESTION 4
Which of the following types of threat attribution deals with the identification of the specific person, society, or a country sponsoring a well-planned and executed intrusion or attack over its target?

A. Nation-state attribution
B. True attribution
C. Campaign attribution
D. Intrusion-set attribution

Answer: B

NEW QUESTION 5
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 6
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 7
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 8
Steve works as an analyst in a UK-based firm. He was asked to perform network monitoring to find any evidence of compromise. During the network monitoring, he came to know that there are multiple logins from different locations in a short time span. Moreover, he also observed certain irregular log in patterns from locations where the organization does not have business relations. This resembles that somebody is trying to steal confidential information.
Which of the following key indicators of compromise does this scenario present?

A. Unusual outbound network traffic
B. Unexpected patching of systems
C. Unusual activity through privileged user account
D. Geographical anomalies

Answer: C

NEW QUESTION 9
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

NEW QUESTION 10
Joe works as a threat intelligence analyst with Xsecurity Inc. He is assessing the TI program by comparing the project results with the original objectives by reviewing project charter. He is also reviewing the list of expected deliverables to ensure that each of those is delivered to an acceptable level of quality.
Identify the activity that Joe is performing to assess a TI program's success or failure.

A. Determining the fulfillment of stakeholders
B. Identifying areas of further improvement
C. Determining the costs and benefits associated with the program
D. Conducting a gap analysis

Answer: D

NEW QUESTION 10
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

NEW QUESTION 12
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

NEW QUESTION 13
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?

A. Search
B. Open
C. Workflow
D. Scoring

Answer: D

NEW QUESTION 16
In a team of threat analysts, two individuals were competing over projecting their own hypotheses on a given malware. However, to find logical proofs to confirm their hypotheses, the threat intelligence manager used a de-biasing strategy that involves learning strategic decision making in the circumstances comprising multistep interactions with numerous representatives, either having or without any perfect relevant information.
Which of the following de-biasing strategies the threat intelligence manager used to confirm their hypotheses?

A. Game theory
B. Machine learning
C. Decision theory
D. Cognitive psychology

Answer: C

NEW QUESTION 17
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

Answer: B

NEW QUESTION 21
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

Answer: D

NEW QUESTION 23
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 26
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?

A. Hydra
B. AutoShun
C. Vanguard enforcer
D. Burp suite

Answer: D

NEW QUESTION 27
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 29
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

Answer: C

NEW QUESTION 31
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?

A. Financial services
B. Social network settings
C. Hacking forums
D. Job sites

Answer: C

NEW QUESTION 36
H&P, 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)

Answer: D

NEW QUESTION 40
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 43
......