EC-Council

Exam Questions 312-85

Certified Threat Intelligence Analyst

NEW QUESTION 1
Which of the following components refers to a node in the network that routes the traffic from a workstation to external command and control server and helps in identification of installed malware in the network?

A. Repeater
B. Gateway
C. Hub
D. Network interface card (NIC)

Answer: B

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
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

NEW QUESTION 4
Lizzy, an analyst, wants to recognize the level of risks to the organization so as to plan countermeasures against cyber attacks. She used a threat modelling methodology where she performed the following stages:
Stage 1: Build asset-based threat profiles
Stage 2: Identify infrastructure vulnerabilities
Stage 3: Develop security strategy and plans
Which of the following threat modelling methodologies was used by Lizzy in the aforementioned scenario?

A. TRIKE
B. VAST
C. OCTAVE
D. DREAD

Answer: C

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
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

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
Daniel is a professional hacker whose aim is to attack a system to steal data and money for profit. He performs hacking to obtain confidential data such as social security numbers, personally identifiable information (PII) of an employee, and credit card information. After obtaining confidential data, he further sells the information on the black market to make money.
Daniel comes under which of the following types of threat actor.

A. Industrial spies
B. State-sponsored hackers
C. Insider threat
D. Organized hackers

Answer: D

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
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 10
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 15
Mr. Bob, a threat analyst, is performing analysis of competing hypotheses (ACH). He has reached to a stage where he is required to apply his analysis skills effectively to reject as many hypotheses and select the best hypotheses from the identified bunch of hypotheses, and this is done with the help of listed evidence. Then, he prepares a matrix where all the screened hypotheses are placed on the top, and the listed evidence for the hypotheses are placed at the bottom.
What stage of ACH is Bob currently in?

A. Diagnostics
B. Evidence
C. Inconsistency
D. Refinement

Answer: A

NEW QUESTION 16
A threat analyst obtains an intelligence related to a threat, where the data is sent in the form of a connection request from a remote host to the server. From this data, he obtains only the IP address of the source and destination but no contextual information. While processing this data, he obtains contextual information stating that multiple connection requests from different geo-locations are received by the server within a short time span, and as a result, the server is stressed and gradually its performance has reduced. He further performed analysis on the information based on the past and present experience and concludes the attack experienced by the client organization.
Which of the following attacks is performed on the client organization?

A. DHCP attacks
B. MAC spoofing attack
C. Distributed Denial-of-Service (DDoS) attack
D. Bandwidth attack

Answer: C

NEW QUESTION 17
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 18
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 19
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 21
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 23
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 24
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

312-85 Practice Exam Features:

* 312-85 Questions and Answers Updated Frequently

* 312-85 Practice Questions Verified by Expert Senior Certified Staff

* 312-85 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 312-85 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 312-85 Practice Test Here