EC-Council

Exam Questions 312-85

Certified Threat Intelligence Analyst

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

   All examinations will be up to date.

* 24/7 Quality Support

   We will provide service round the clock.

* 100% Pass Rate

   Our guarantee that you will pass the exam.

* Unique Gurantee

   If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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?

A. Mediated trust
B. Mandated trust
C. Direct historical trust
D. Validated trust

Answer: D

NEW QUESTION 2
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 3
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 4
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 data. 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?

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

Answer: C

NEW QUESTION 5
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 6
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 7
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 8
A team of threat intelligence analysts is performing threat analysis on malware, and each of them has come up with their own theory and evidence to support their theory on a given malware.
Now, to identify the most consistent theory out of all the theories, which of the following analytic processes must threat intelligence manager use?

A. Threat modelling
B. Application decomposition and analysis (ADA)
C. Analysis of competing hypotheses (ACH)
D. Automated technical analysis

Answer: C

NEW QUESTION 9
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 10
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 10
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 13
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 18
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?

A. OPSEC
B. ISAC
C. OSINT
D. SIGINT

Answer: C

NEW QUESTION 21
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 26
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 31
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 35
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 39
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 42
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 44
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 48
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 49
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 53
......

Relate Links

100% Pass Your 312-85 Exam with Exambible Prep Materials

https://www.exambible.com/312-85-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/