2023 100% Free 312-85 Daily Practice Exam With 50 Questions [Q26-Q49

2023 100% Free 312-85 Daily Practice Exam With 50 Questions
312-85 exam torrent ECCouncil study guide

The CTIA certification exam is an essential certification for professionals who want to demonstrate their expertise in the field of threat intelligence analysis. Certified Threat Intelligence Analyst certification exam covers various topics such as threat intelligence analysis, threat modeling, threat assessment, and threat communication. Certified Threat Intelligence Analyst certification demonstrates that the candidate is committed to staying up-to-date with the latest developments in the field of cybersecurity and is dedicated to providing the best services to their clients.

Q26. 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?
* Diagnostics

* Evidence
* Inconsistency
* Refinement

Q27. 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.
* Determining the fulfillment of stakeholders
* Identifying areas of further improvement
* Determining the costs and benefits associated with the program
* Conducting a gap analysis

Q28. 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?
* Unknown unknowns
* Unknowns unknown
* Known unknowns
* Known knowns

Q29. 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?
* Unusual outbound network traffic
* Unexpected patching of systems
* Unusual activity through privileged user account
* Geographical anomalies

Q30. 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?
* Repeater
* Gateway
* Hub
* Network interface card (NIC)

Q31. 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.
* Alison should use SmartWhois to extract the required website information.
* Alison should use https://archive.org to extract the required website information.
* Alison should run the Web Data Extractor tool to extract the required website information.
* Alison should recover cached pages of the website from the Google search engine cache to extract the required website information.

Q32. 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?
* Game theory
* Machine learning
* Decision theory
* Cognitive psychology

Q33. 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.
* Operational threat intelligence analysis
* Technical threat intelligence analysis
* Strategic threat intelligence analysis
* Tactical threat intelligence analysis

Q34. 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

Q35. 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)

* 1–>9–>2–>8–>3–>7–>4–>6–>5
* 3–>4–>5–>2–>1–>9–>8–>7–>6
* 1–>2–>3–>4–>5–>6–>9–>8–>7
* 1–>2–>3–>4–>5–>6–>7–>8–>9

Q36. 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.
* Active data collection
* Passive data collection
* Exploited data collection
* Raw data collection

Q37. Walter and Sons Company has faced major cyber attacks and lost confidential dat a. The company has decided to concentrate more on the security rather than other resources. Therefore, they hired Alice, a threat analyst, to perform data analysis. Alice was asked to perform qualitative data analysis to extract useful information from collected bulk data.

Which of the following techniques will help Alice to perform qualitative data analysis?
* Regression analysis, variance analysis, and so on
* Numerical calculations, statistical modeling, measurement, research, and so on.
* Brainstorming, interviewing, SWOT analysis, Delphi technique, and so on
* Finding links between data and discover threat-related information

Q38. 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

Q39. 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?
* Providers of threat data feeds
* Providers of threat indicators
* Providers of comprehensive cyber-threat intelligence
* Providers of threat actors

Q40. 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

Q41. 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

Q42. 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

Q43. 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.
* Industrial spies
* State-sponsored hackers
* Insider threat
* Organized hackers

Q44. 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

Q45. 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?
* Advisories
* Strategic reports
* Detection indicators
* Low-level data

Q46. 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?
* TRIKE
* VAST
* OCTAVE
* DREAD

Q47. 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?
* Sam used unreliable intelligence sources.
* Sam used data without context.
* Sam did not use the proper standardization formats for representing threat data.
* Sam did not use the proper technology to use or consume the information.

Q48. 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