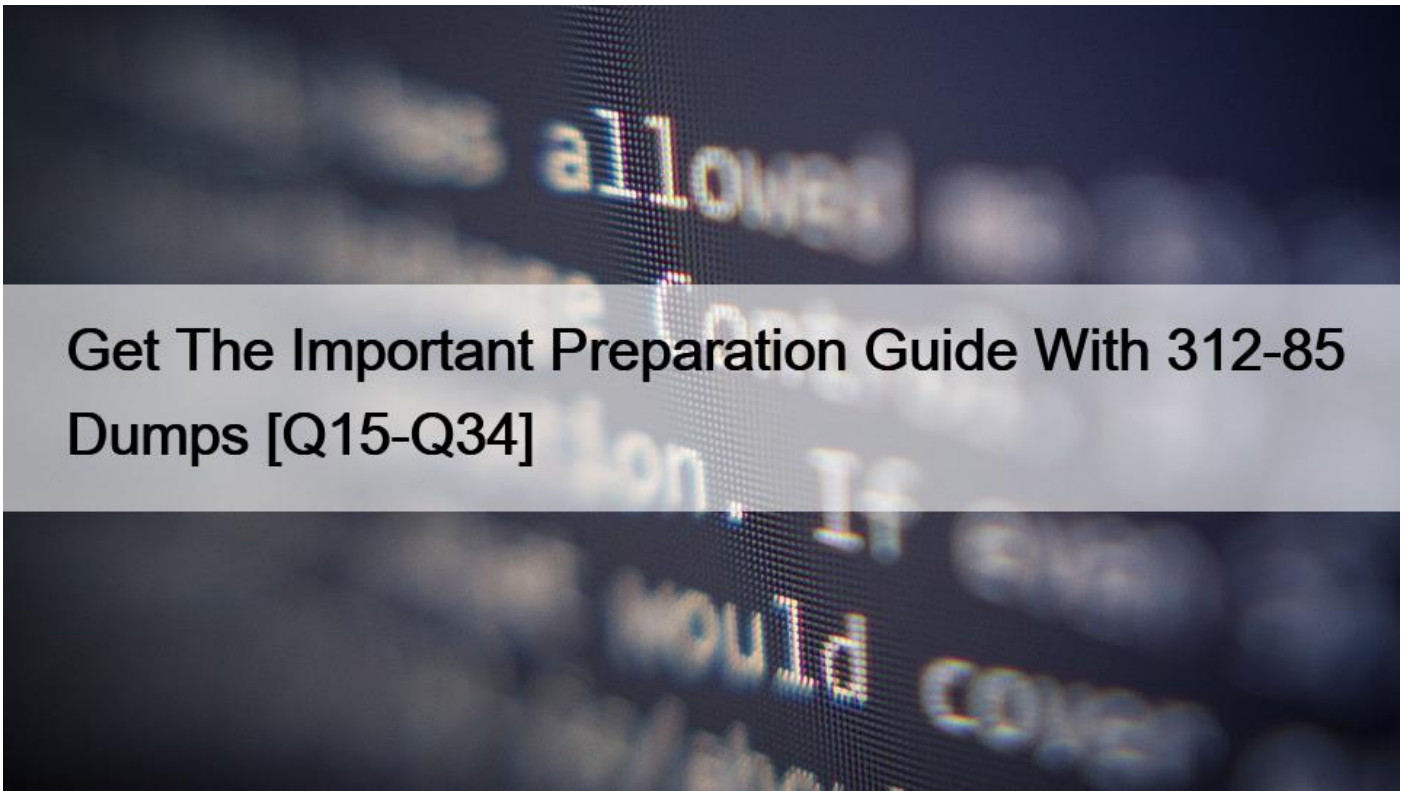
Get The Important Preparation Guide With 312-85 Dumps [Q15-Q34



Get The Important Preparation Guide With 312-85 Dumps Get Totally Free Updates on 312-85 Dumps PDF Questions

ECCouncil 312-85 Exam Syllabus Topics:

TopicDetailsTopic 1- Understanding Threat Intelligence Data Collection and Acquisition- Overview of Threat Intelligence Collection ManagementTopic 2- Overview of Fine-Tuning Threat Analysis- Understanding Threat Intelligence Evaluation
Topic 3- Understanding Indicators of Compromise- Understanding Advanced Persistent ThreatsTopic 4- Understanding Cyber Threat Intelligence- Understanding IntelligenceTopic 5- Understanding Requirements Analysis- Building a Threat Intelligence TeamTopic 6- Cyber Threats and Kill Chain Methodology- Understanding Cyber Kill ChainTopic 7- Overview of Threat Intelligence Lifecycle and Frameworks- Introduction to Threat IntelligenceTopic 8- Overview of Intelligence Sharing Acts and Regulations- Understanding the Threat Analysis ProcessTopic 9- Understanding Threat Intelligence Sharing Platforms- Understanding Data Processing and ExploitationTopic 10- Overview of Threat Intelligence Sharing- Requirements, Planning, Direction, and ReviewTopic 11- Understanding Organization's Current Threat Landscape- Reviewing Threat Intelligence ProgramTopic 12- Overview of Threat Intelligence Feeds and Sources- Overview of Threat Intelligence Data Collection

Q15. 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

Q16. 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

Q17. 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?
* HighCharts
* SIGVERIF
* Threat grid
* TC complete

Q18. 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

Q19. 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?
* Threat modelling
* Application decomposition and analysis (ADA)
* Analysis of competing hypotheses (ACH)
* Automated technical analysis

Q20. 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

Q21. 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

Q22. 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

Q23. Which of the following characteristics of APT refers to numerous attempts done by the attacker to gain entry to the target’s network?
* Risk tolerance
* Timeliness
* Attack origination points
* Multiphased

Q24. 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

Q25. 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

Q26. 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

Q27. 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?
* Reconnaissance
* Installation
* Weaponization
* Exploitation

Q28. 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

Q29. 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?
* Strategic threat intelligence
* Tactical threat intelligence
* Technical threat intelligence
* Operational threat intelligence

Q30. 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.
* Level 2: increasing CTI capabilities
* Level 3: CTI program in place
* Level 1: preparing for CTI
* Level 0: vague where to start

Q31. Kim, an analyst, is looking for an intelligence-sharing platform to gather and share threat information from a variety of sources. He wants to use this information to develop security policies to enhance the overall security posture of his organization.

Which of the following sharing platforms should be used by Kim?
* Cuckoo sandbox
* OmniPeek
* PortDroid network analysis
* Blueliv threat exchange network

Q32. 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

Q33. 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.

Q34. 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