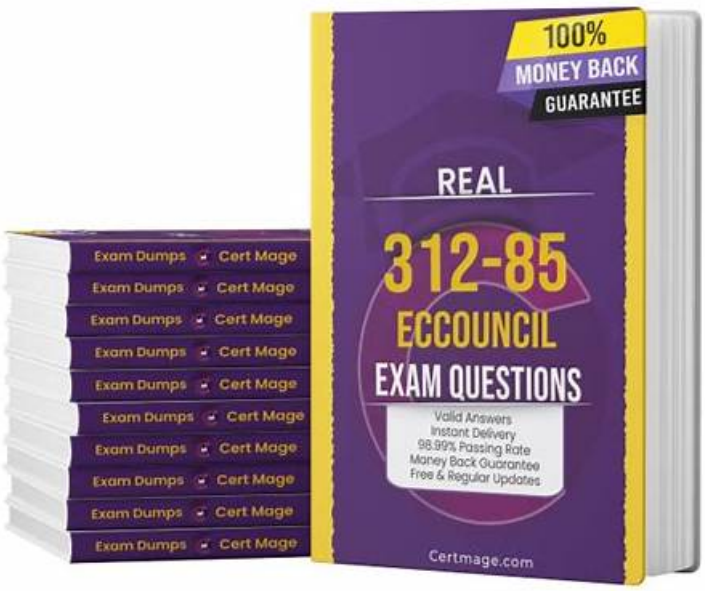
Extraordinary ECCouncil 312-85 Exam Dumps To Pass The 312-85 Exam



DOWNLOAD the newest PrepPDF 312-85 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1SAA9lXp9MrpDxPS1y70HfiIqBUMbbtI1

Customizable Certified Threat Intelligence Analyst (312-85) practice tests allow users set the time and 312-85 questions according to their needs. Certified Threat Intelligence Analyst (312-85) Practice exams simulate the real test so applicants can prepare as per the actual exam's pressure and handle it in the final test. PrepPDF has a team of professionals who update the Certified Threat Intelligence Analyst (312-85) practice material daily so the user can get the full out of it and pass Certified Threat Intelligence Analyst (312-85) certification exam pretty easily.

The Certified Threat Intelligence Analyst (CTIA) certification exam is a professional qualification designed to equip individuals with the skills, knowledge, and abilities to analyze and respond to cyber threats effectively. Offered by the ECCouncil, the CTIA certification exam covers a range of topics related to threat intelligence, including threat identification, analysis, response, and dissemination. 312-85 Exam is designed for cybersecurity professionals, including incident responders, security analysts, threat intelligence analysts, and other professionals in the cybersecurity industry.

The Certified Threat Intelligence Analyst (CTIA) is a certification exam offered by the EC-Council. The CTIA certification is a professional-level certification that is designed to validate the skills and knowledge of individuals who work in the field of threat intelligence analysis. The CTIA exam is designed to test the candidate's ability to collect, analyze, and disseminate threat intelligence data from various sources.

>> 312-85 Valid Test Vce Free <<

312-85 Latest Test Online & 312-85 Relevant Questions

I would like to find a different job, because I am tired of my job and present life. Do you have that idea? How to get a better job? Are you interested in IT industry? Do you want to prove yourself through IT? If you want to work in the IT field, it is essential to register IT certification exam and get the certificate. The main thing for you is to take IT certification exam that is accepted commonly which will help you to open a new journey. And you must be familiar with ECCouncil 312-85 Certification test. To obtain the certificate will help you to find a better job. What? Do you have no confidence to take the exam? It doesn't matter that you can use

our PrepPDF dumps.

The Certified Threat Intelligence Analyst (CTIA) certification is offered by the International Council of Electronic Commerce Consultants (EC-Council). It is specifically designed for individuals who wish to specialize in the field of threat intelligence. The CTIA certification is globally recognized, and it is an essential credential for professionals who work in the field of cybersecurity. Certified Threat Intelligence Analyst certification exam tests candidates on key concepts related to threat intelligence, including threat modeling, data collection, and analysis.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q22-Q27):

NEW QUESTION # 22
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. Amber
- B. White
- C. Green
- D. Red

Answer: C

NEW QUESTION # 23
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. Inconsistency
- B. Diagnostics
- C. Evidence
- D. Refinement

Answer: B

NEW QUESTION # 24
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 actors
- C. Providers of threat indicators
- D. Providers of comprehensive cyber-threat intelligence

Answer: D

Explanation:
The information Sarah is gathering, which includes collections of validated and prioritized threat indicators along with detailed technical analysis of malware samples, botnets, DDoS methods, and other malicious tools, indicates that she is obtaining this intelligence from providers of comprehensive cyber-threat intelligence.
These providers offer a holistic view of the threat landscape, combining tactical and operational threat data with in-depth analysis and context, enabling security teams to make informed decisions and strategically enhance their defenses.
References:
"Cyber Threat Intelligence Providers: How to Choose the Right One for Your Organization," by CrowdStrike

"The Role of Comprehensive Cyber Threat Intelligence in Effective Cybersecurity Strategies," by FireEye

NEW QUESTION # 25
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 afterperforming 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. Low-level data
- D. Detection indicators

Answer: C

Explanation:
The network administrator collected log files generated by a traffic monitoring system, which falls under the category of low-level data. This type of data might not appear useful at first glance but can reveal significant insights about network activity and potential threats upon thorough analysis. Low-level data includes raw logs, packet captures, and other granular details that, when analyzed properly, can help detect anomalous behaviors or indicators of compromise within the network. This type of information is essential for detection and response efforts, allowing security teams to identify and mitigate threats in real-time.References:
* "Network Forensics: Tracking Hackers through Cyberspace," by Sherri Davidoff and Jonathan Ham, Prentice Hall
* "Real-Time Detection of Anomalous Activity in Dynamic, Heterogeneous Information Systems," IEEE Transactions on Information Forensics and Security

NEW QUESTION # 26
Marie, a threat analyst at an organization named TechSavvy, was asked to perform operational threat intelligence analysis to get contextual information about security events and incidents.
Which of the following sources does Marie need to use to perform operational threat intelligence analysis?

- A. OSINT, security industry white papers, human contacts
- B. Activity-related attacks, social media sources, chat room conversations
- C. Attack group reports, attack campaign reports, incident reports, malware samples
- D. Malware indicators, network indicators, e-mail indicators

Answer: C

Explanation:
Operational Threat Intelligence focuses on providing actionable insights about ongoing attacks, campaigns, or threat actors. It bridges the gap between high-level strategic intelligence and low-level technical intelligence.
It includes detailed, contextual information about how and why an attack is happening, who is behind it, and what tools and tactics they are using. Analysts rely on reports and data that describe current or recent attack campaigns, group activities, and malware operations.
Typical Sources of Operational Threat Intelligence:
* Attack group reports: Identify specific threat actors, their motivations, targets, and past operations.
* Attack campaign reports: Provide information about organized and ongoing attack campaigns targeting certain sectors or geographies.
* Incident reports: Offer real-world case studies and patterns of attacks that have already occurred.
* Malware samples: Help analysts understand malware functionality, distribution methods, and associated threat groups.
These sources provide contextual and actionable information that help operational analysts improve detection and response during active threat situations.
Why the Other Options Are Incorrect:
* B. Malware indicators, network indicators, e-mail indicators:These are sources of technical threat intelligence, which deals with atomic-level data such as IP addresses, URLs, and file hashes.
* C. Activity-related attacks, social media sources, chat room conversations:These are examples of sources used for social media or OSINT collection, not operational analysis.
* D. OSINT, security industry white papers, human contacts:These are sources used for strategic threat intelligence, focusing on long-term trends and organizational risk assessment.
Conclusion:

Operational threat intelligence relies on actionable, campaign-specific sources such as attack group reports, incident reports, and malware samples to provide detailed context for active threats.
Final Answer: A. Attack group reports, attack campaign reports, incident reports, malware samples Explanation Reference (Based on CTIA Study Concepts):
According to CTIA, operational threat intelligence provides in-depth analysis of ongoing or recent campaigns, utilizing reports and samples that describe adversary tools, targets, and motivations.

NEW QUESTION # 27
.....