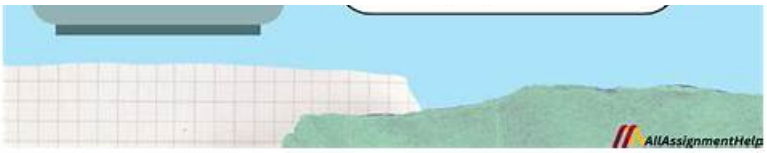
Help You Learn, Prepare, and Practice for 312-85 exam success



BONUS!!! Download part of DumpsKing 312-85 dumps for free: https://drive.google.com/open?id=16UVfC6t-JPAACES7GazmqB3RgvvflNSh

Our 312-85 study practice guide takes full account of the needs of the real exam and conveniences for the clients. Our 312-85 certification questions are close to the real exam and the questions and answers of the test bank cover the entire syllabus of the real exam and all the important information about the exam. Our 312-85 Learning Materials can stimulate the real exam's environment to make the learners be personally on the scene and help the learners adjust the speed when they attend the real 312-85 exam.

ECCouncil 312-85 Certification Exam is a vendor-neutral certification that is recognized globally. It is an advanced-level certification that requires candidates to have a thorough understanding of the latest threat intelligence techniques and tools. Certified Threat Intelligence Analyst certification covers various topics such as threat intelligence planning, collection and analysis, cyber threat intelligence, and threat intelligence operations. Candidates are expected to have a good understanding of these topics to pass the certification exam.

The CTIA certification exam is a comprehensive exam that covers a range of topics related to threat intelligence. 312-85 exam consists of 100 multiple-choice questions that must be completed within four hours. 312-85 exam covers topics such as the intelligence cycle, cyber threat landscape, threat actors and their motivations, intelligence gathering techniques, and threat analysis and response. The CTIA certification exam is an excellent way for cybersecurity professionals to demonstrate their expertise in threat intelligence and to enhance their career prospects in the cybersecurity industry.

The Certified Threat Intelligence Analyst certification is ideal for professionals who work in the field of cybersecurity, such as security analysts, threat hunters, and incident responders. It is also suitable for individuals who are interested in pursuing a career in threat intelligence. Certified Threat Intelligence Analyst certification demonstrates a candidate's commitment to staying up-to-date with the latest trends and developments in the field of cybersecurity.

>> 312-85 Vce Exam <<

User-Friendly ECCouncil 312-85 Exam Questions in PDF Format

It can be said that all the content of the 312-85 prepare questions are from the experts in the field of masterpieces, and these are understandable and easy to remember, so users do not have to spend a lot of time to remember and learn our 312-85 exam questions. It takes only a little practice on a daily basis to get the desired results. Especially in the face of some difficult problems, the user does not need to worry too much, just learn the 312-85 Practice Guide provide questions and answers, you can simply pass the 312-85 exam.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q80-Q85):

NEW QUESTION # 80
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. Search and exfiltration
- B. Persistence
- C. Initial intrusion
- D. Expansion

Answer: D

Explanation:
The phase described where John, after gaining initial access, is attempting to obtain administrative credentials to further access

systems within the network, is known as the 'Expansion' phase of an Advanced Persistent Threat (APT) lifecycle. This phase involves the attacker expanding their foothold within the target's environment, often by escalating privileges, compromising additional systems, and moving laterally through the network. The goal is to increase control over the network and maintain persistence for ongoing access.
This phase follows the initial intrusion and sets the stage for establishing long-term presence and eventual data exfiltration or other malicious objectives.References:
* MITRE ATT&CK Framework, specifically the tactics related to Credential Access and Lateral Movement
* "APT Lifecycle: Detecting the Undetected," a whitepaper by CyberArk

NEW QUESTION # 81
Which of the following types of threat attribution deals with the identification of the specific person, society, or a country sponsoring a well-planned and executed intrusion or attack over its target?

- A. Intrusion-set attribution
- B. Nation-state attribution
- C. True attribution
- D. Campaign attribution

Answer: C

Explanation:
True attribution in the context of cyber threats involves identifying the actual individual, group, or nation- state behind an attack or intrusion. This type of attribution goes beyond associating an attack with certain tactics, techniques, and procedures (TTPs) or a known group and aims to pinpoint the real-world entity responsible. True attribution is challenging due to the anonymity of the internet and the use of obfuscation techniques by attackers, but it is crucial for understanding the motive behind an attack and for forming appropriate responses at diplomatic, law enforcement, or cybersecurity levels.
References:
"Attribution of Cyber Attacks: A Framework for an Evidence-Based Analysis" by Jason Healey
"The Challenges of Attribution in Cyberspace" in the Journal of Cyber Policy

NEW QUESTION # 82
You are a cybersecurity analyst working at a financial institution. An unusual pattern of financial transactions was detected, suggesting potential fraud or money laundering. What specific type of threat intelligence would you rely on to analyze these financial activities and identify potential risks?

- A. FININT
- B. CHIS
- C. TECHINT
- D. OSINT

Answer: A

Explanation:
FININT (Financial Intelligence) refers to the collection, processing, and analysis of financial transaction data to identify suspicious or illicit activities such as fraud, money laundering, terrorist financing, or financial crimes.
In this scenario, the analyst is investigating unusual financial transaction patterns, which is exactly the purpose of financial intelligence.
Key Features of FININT:
* Focuses on financial data sources, including transaction records, wire transfers, and account statements.
* Helps detect illicit financial flows or abnormal transaction behaviors.
* Used by banks, financial institutions, and government agencies to identify and prevent financial crimes.
* Often shared with intelligence agencies and regulatory bodies to support counter-fraud and anti-money laundering operations.
Why the Other Options Are Incorrect:
* A. OSINT:Refers to publicly available information such as websites, news, or social media. It is not specific to financial transaction data.
* B. CHIS:Refers to human intelligence sources obtained through personal or covert interaction, not financial data analysis.
* C. TECHINT:Refers to intelligence gathered from technical sources such as sensors or electronic systems, not financial records.
Conclusion:
The correct intelligence type used to analyze suspicious financial transactions is FININT (Financial Intelligence).
Final Answer: D. FININT

Explanation Reference (Based on CTIA Study Concepts):
As per CTIA threat intelligence classifications, FININT involves collecting and analyzing financial data to detect and mitigate fraudulent or criminal activities.

NEW QUESTION # 83
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 on latest vulnerabilities, threat actors, and their tactics, techniques, and procedures (TTPs)
- B. Intelligence extracted latest attacks analysis on similar organizations, which includes details about latest threats and TTPs
- C. Intelligence that reveals risks related to various strategic business decisions
- D. Intelligence related to increased attacks targeting a particular software or operating system vulnerability

Answer: A

NEW QUESTION # 84
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?

- A. Advisories
- B. Low-level data
- C. Strategic reports
- D. Detection indicators

Answer: B

NEW QUESTION # 85
.....

If you are finding a study material to prepare your exam, our material will end your search. Our 312-85 exam torrent has a high quality that you can't expect. I think our 312-85 prep torrent will help you save much time, and you will have more free time to do what you like to do. I can guarantee that you will have no regrets about using our 312-85 Test Braindumps When the time for action arrives, stop thinking and go in, try our 312-85 exam torrent, you will find our products will be a very good choice for you to pass your exam and get you certificate in a short time.

download exam materials for free through ➤ www.prepawayete.com □ □New 312-85 Exam Sample

- Valid 312-85 Exam Answers □ 312-85 Reliable Braindumps Free □□ 312-85 Reliable Dump □ Simply search for " 312-85 " for free download on ➤ www.pdfvce.com □ □312-85 Most Reliable Questions
- 312-85 Exam Vce Exam– Fantastic 312-85 Valid Exam Dumps Pass Success □ Search for 「 312-85 」 and easily obtain a free download on □ www.examcollectionpass.com □ □312-85 Simulations Pdf
- aliciaxjtr696721.wikimidpoint.com, darzayan.com, karimaeka941202.hamachiwiki.com, bookmarks4seo.com, karimbgbr562926.get-blogging.com, marchjah708040.prublogger.com, cecilyzcik465995.wikikali.com, lancenmds566741.blogtov.com, jadagnhg042963.dreamyblogs.com, jonasmvhs979881.thelateblog.com, Disposable vapes

P.S. Free & New 312-85 dumps are available on Google Drive shared by DumpsKing: https://drive.google.com/open?id=16UVfC6t-JPAACES7GazmqB3RgvvflNSh