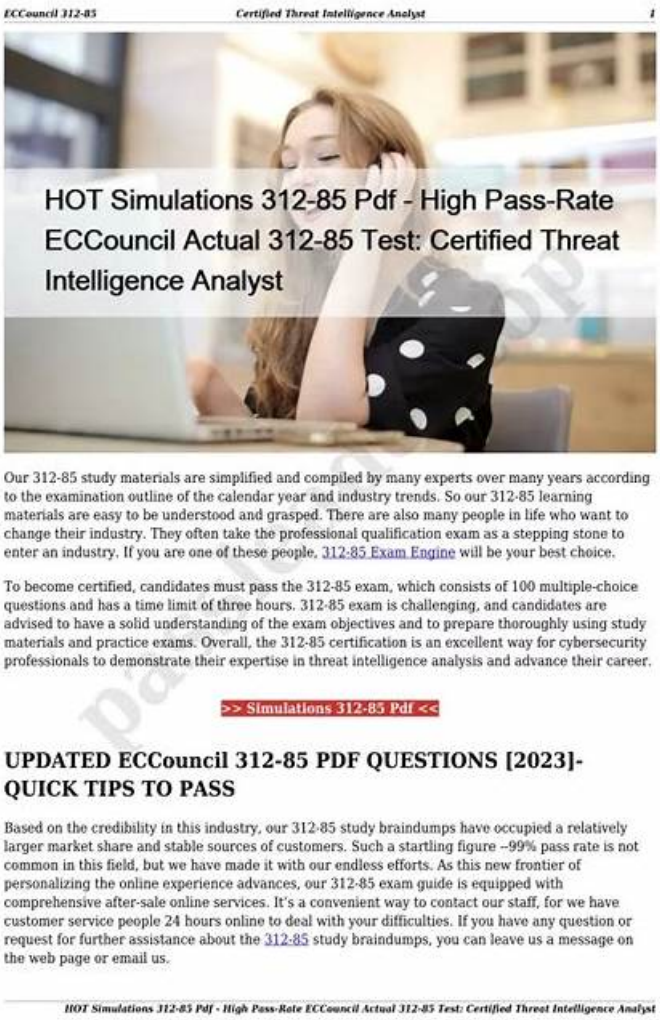
Pass Guaranteed Quiz ECCouncil - Pass-Sure 312-85 - Test Certified Threat Intelligence Analyst Question



BONUS!!! Download part of Test4Engine 312-85 dumps for free: https://drive.google.com/open?id=1EPGIjXGJWxsDNSzUsjbjOfDd6QN6zJPI

All-in-One Exam Guide Practice To your 312-85 Exam. To meet this objective Test4Engine is offering valid, updated, and real 312-85 exam practice test questions in their formats.. Download 312-85 study guide pdf, pass Certified Threat Intelligence Analyst exam with full refund guarantee! Success ECCouncil exam with 312-85 Exam Questions which has high pass rate. Use free 312-85 certification questions to gain a good test result.

The EC-Council Certified Threat Intelligence Analyst (CTIA) certification exam is designed to test the knowledge and skills of individuals who are interested in a career in threat intelligence. 312-85 Exam will validate the candidate's knowledge in identifying and combating cybersecurity threats, as well as the ability to provide effective threat intelligence analysis to organizations. The CTIA certification exam is an advanced-level exam and requires a deep understanding of cybersecurity and threat intelligence concepts.

The Certified Threat Intelligence Analyst (CTIA) certification is an intermediate-level certification, intended for individuals who already have a basic understanding of cybersecurity concepts. Certified Threat Intelligence Analyst certification covers a broad range of topics, including threat intelligence, data analysis, threat modeling, and threat hunting. The CTIA certification ensures that individuals are equipped with the skills and knowledge necessary to detect, analyze, and respond to cyber threats in real-time.

>> Test 312-85 Question <<

ECCouncil 312-85 Web-Based Practice Exam Questions Software

You can use this ECCouncil 312-85 version on any operating system, and this software is accessible through any browser like Opera, Safari, Chrome, Firefox, and IE. You can easily assess yourself with the help of our 312-85 practice software, as it records all your previous results for future use.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q76-Q81):

NEW QUESTION # 76
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. Workflow
- C. Scoring
- D. Open

Answer: C

Explanation:
Incorporating a scoring feature in a Threat Intelligence (TI) platform allows SecurityTech Inc. to evaluate and prioritize intelligence sources, threat actors, specific types of attacks, and the organization's digital assets based on their relevance and threat level to the organization. This prioritization helps in allocating resources more effectively, focusing on protecting critical assets and countering the most significant threats. A scoring system can be based on various criteria such as the severity of threats, the value of assets, the reliability of intelligence sources, and the potential impact of threat actors or attack vectors. By quantifying these elements, SecurityTech Inc. can make informed decisions on where to invest its limited funds to enhance its security posture most effectively.References:
* "Designing and Building a Cyber Threat Intelligence Capability" by the SANS Institute
* "Threat Intelligence: What It Is, and How to Use It Effectively" by Gartner

NEW QUESTION # 77
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. Persistence
- B. Expansion
- C. Search and exfiltration
- D. Initial intrusion

Answer: B

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 # 78
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?

- A. Normalization
- B. Sandboxing
- C. Data visualization
- D. Convenience sampling

Answer: A

NEW QUESTION # 79
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 activity through privileged user account
- B. Geographical anomalies
- C. Unexpected patching of systems
- D. Unusual outbound network traffic

Answer: B

Explanation:
The scenario described by Steve's observations, where multiple logins are occurring from different locations in a short time span, especially from locations where the organization has no business relations, points to
'Geographical anomalies' as a key indicator of compromise (IoC). Geographical anomalies in logins suggest unauthorized access attempts potentially made by attackers using compromised credentials. This is particularly suspicious when the locations of these logins do not align with the normal geographical footprint of the organization's operations or employee locations. Monitoring for such anomalies can help in the early detection of unauthorized access and potential data breaches.
References:
SANS Institute Reading Room, "Indicators of Compromise: Reality's Version of the Minority Report"
"Identifying Indicators of Compromise" by CERT-UK

NEW QUESTION # 80
Tracy works as a CISO in a large multinational company. She consumes threat intelligence to understand the changing trends of cyber security. She requires intelligence to understand the current business trends and make appropriate decisions regarding new technologies, security budget, improvement of processes, and staff.
The intelligence helps her in minimizing business risks and protecting the new technology and business initiatives.
Identify the type of threat intelligence consumer is Tracy.

- A. Operational users
- B. Tactical users
- C. Technical users
- D. Strategic users

Answer: D

Explanation:
Tracy, as a Chief Information Security Officer (CISO), requires intelligence that aids in understanding broader business and cybersecurity trends, making informed decisions regarding new technologies, security budgets, process improvements, and staffing. This need aligns with the role of a strategic user of threat intelligence. Strategic users leverage intelligence to guide long-term planning and decision-making, focusing on minimizing business risks and safeguarding against emerging threats to new technology and business initiatives. This type of intelligence is less about the technical specifics of individual threats and more about understanding the overall threat landscape, regulatory environment, and industry trends to inform high-level strategy and policy.
References:

"The Role of Strategic Intelligence in Cybersecurity," Journal of Cybersecurity Education, Research and Practice
"Cyber Threat Intelligence and the Lessons from Law Enforcement," by Robert M. Lee and David Bianco, SANS Institute Reading Room

NEW QUESTION # 81

......

It is well known that the best way to improve your competitive advantages in this modern world is to increase your soft power, such as graduation from a first-tier university, fruitful experience in a well-known international company, or even possession of some globally recognized 312-85 certifications, which can totally help you highlight your resume and get a promotion in your workplace to a large extend. As a result, our 312-85 Study Materials raise in response to the proper time and conditions while an increasing number of people are desperate to achieve success and become the elite.

Instant 312-85 Access: https://www.test4engine.com/312-85_exam-latest-braindumps.html

- 312-85 Exam Torrent □ 312-85 Exam Dumps Collection □ Latest Study 312-85 Questions □ Open ➽ www.prepawaypdf.com □ and search for ➠ 312-85 □ to download exam materials for free □312-85 Reliable Study Plan
- Test 312-85 Questions Answers □ 312-85 Valid Exam Format □ Latest Study 312-85 Questions □ Download 【 312-85 】 for free by simply searching on ▶ www.pdfvce.com ◀ □312-85 Reliable Exam Simulator
- 312-85 Dump □ Latest Study 312-85 Questions □ 312-85 Reliable Braindumps □ Download [312-85] for free by simply entering ☀ www.examcollectionpass.com □☀□ website □312-85 Reliable Exam Simulator
- 312-85 Reliable Exam Simulator □ Training 312-85 For Exam □ Latest Study 312-85 Questions ✍ Open （ www.pdfvce.com ） and search for 「 312-85 」 to download exam materials for free □312-85 Dump
- 2026 312-85: High Pass-Rate Test Certified Threat Intelligence Analyst Question □ □ www.practicevce.com □ is best website to obtain □ 312-85 □ for free download □312-85 Reliable Exam Review
- Latest Study 312-85 Questions □ 312-85 Exam Dumps Collection □ Exam 312-85 Collection □ Search for " 312-85 " and download exam materials for free through ▶ www.pdfvce.com ◀ □312-85 Valid Exam Format
- ECCouncil - High Hit-Rate 312-85 - Test Certified Threat Intelligence Analyst Question ♥ The page for free download of ⇒ 312-85 ⇐ on ▶ www.practicevce.com ◀ will open immediately □312-85 Dump
- Test 312-85 Questions Answers □ 312-85 Exam Dumps Collection □ Reliable 312-85 Real Test □ Enter { www.pdfvce.com } and search for □ 312-85 □ to download for free □312-85 Dump
- 312-85 Reliable Braindumps □ Training 312-85 For Exam □ 312-85 Reliable Exam Simulator □ Download ➠ 312-85 □ for free by simply searching on □ www.practicevce.com □ ❣312-85 Exam Dumps Collection
- 312-85 Valid Exam Question □ Dumps 312-85 Torrent □ 312-85 Valid Exam Question □ Open 《 www.pdfvce.com 》 enter ▷ 312-85 ◁ and obtain a free download □312-85 Exam Torrent
- Exam 312-85 Collection □ New 312-85 Braindumps Free □ 312-85 Valid Exam Question □ Open website ▷ www.easy4engine.com ◁ and search for ⇒ 312-85 ⇐ for free download □New 312-85 Braindumps Free
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes

DOWNLOAD the newest Test4Engine 312-85 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1EPGIjXGJWxsDNSzUsjbjOfDd6QN6zJPI