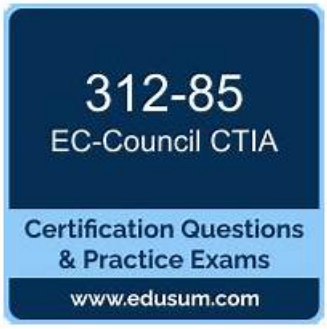
312-85 Study Guide Pdf - 312-85 Exam Braindumps



BONUS!!! Download part of Test4Sure 312-85 dumps for free: https://drive.google.com/open?id=1O4ImQcU1NESr_MWhQYP6639Ki4WZVbu9

At the information age, knowledge is wealth as well as productivity. All excellent people will become outstanding one day as long as one masters skill. In order to train qualified personnel, our company has launched the 312-85 Study Materials for job seekers. We are professional to help tens of thousands of the candidates get their 312-85 certification with our high quality of 312-85 exam questions and live a better life.

With all this reputation, our company still take customers first, the reason we become successful lies on the professional expert team we possess , who engage themselves in the research and development of our 312-85 learning guide for many years. We here promise you that our 312-85 certification material is the best in the market, which can definitely exert positive effect on your study. Our Certified Threat Intelligence Analyst learn tool create a kind of relaxing leaning atmosphere that improve the quality as well as the efficiency, on one hand provide conveniences, on the other hand offer great flexibility and mobility for our customers. That's the reason why you should choose us.

>> 312-85 Study Guide Pdf <<

First-Grade ECCouncil 312-85: Certified Threat Intelligence Analyst Study Guide Pdf - Pass-Sure Test4Sure 312-85 Exam Braindumps

Studying from an updated practice material is necessary to get success in the ECCouncil 312-85 certification test on the first try. If you don't adopt this strategy, you will not be able to clear the Certified Threat Intelligence Analyst (312-85) examination. Failure in the Certified Threat Intelligence Analyst (312-85) test will lead to loss of confidence, time, and money.

ECCouncil 312-85: Certified Threat Intelligence Analyst exam is an essential certification for professionals in the field of cybersecurity. Certified Threat Intelligence Analyst certification validates the candidate's knowledge and skills in identifying, assessing, and mitigating threats to an organization's infrastructure, data, and personnel. Certified Threat Intelligence Analyst certification is highly valued in the industry, and it is an excellent way to demonstrate a commitment to staying up-to-date with the latest trends and developments in the field of cybersecurity.

The CTIA certification is an excellent choice for professionals who want to demonstrate their expertise in threat intelligence analysis.

It is a highly respected certification that is recognized by employers worldwide, and it can help professionals advance their careers and increase their earning potential.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q58-Q63):

NEW QUESTION # 58
Jack is a professional hacker who wants to perform remote exploitation on the target system of an organization. He established a two-way communication channel between the victim's system and his server.
He used encryption techniques to hide the presence of a communication channel on a victim's system and further applied privilege escalation techniques to exploit the system.
What phase of the cyber kill chain methodology is Jack currently in?

- A. Reconnaissance
- B. Delivery
- C. Weaponization
- D. Command and Control

Answer: D

Explanation:
In the Cyber Kill Chain model, the Command and Control (C2) phase refers to the stage where the attacker establishes a communication channel between the compromised system and their own server to maintain remote control, issue commands, and exfiltrate data.
In the given scenario, Jack has already compromised the system and set up a two-way communication link, which is encrypted to avoid detection. This activity is characteristic of the Command and Control phase.
Key Characteristics of the Command and Control Phase:
* The attacker establishes remote communication with the compromised host.
* Encryption or obfuscation methods are used to hide the channel.
* The attacker uses this channel to send further commands, escalate privileges, and execute malicious actions.
* Typical tools: Remote Access Trojans (RATs), backdoors, and tunneling techniques.
Why the Other Options Are Incorrect:
* B. Weaponization:This phase involves creating or configuring the malicious payload or exploit (e.g., binding malware to a document or executable). It occurs before the attack delivery.
* C. Reconnaissance:The attacker gathers information about the target (network structure, vulnerabilities) before launching an attack.
* D. Delivery:This phase involves transmitting the weaponized payload to the target through methods such as email attachments, infected links, or USB drives.
Conclusion:
By establishing an encrypted communication channel and controlling the victim's system remotely, Jack is in the Command and Control phase of the Cyber Kill Chain.
Final Answer: A. Command and Control
Explanation Reference (Based on CTIA Study Concepts):
As defined in CTIA materials under "Adversary Tactics, Techniques, and Procedures (TTPs)" and "Cyber Kill Chain Stages," the Command and Control phase involves creating and maintaining communication between compromised hosts and attacker infrastructure for persistent access and control.

NEW QUESTION # 59
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. Unexpected patching of systems
- B. Geographical anomalies
- C. Unusual outbound network traffic
- D. Unusual activity through privileged user account

Answer: D

NEW QUESTION # 60
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. Unexpected patching of systems
- B. Unusual activity through privileged user account
- C. Unusual outbound network traffic
- D. Geographical anomalies

Answer: D

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 # 61
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?

- A. Sam did not use the proper technology to use or consume the information.
- B. Sam used data without context.
- C. Sam used unreliable intelligence sources.
- D. Sam did not use the proper standardization formats for representing threat data.

Answer: C

Explanation:
Sam's mistake was using threat intelligence from sources that he did not verify for reliability. Relying on intelligence from unverified or unreliable sources can lead to the incorporation of inaccurate, outdated, or irrelevant information into the organization's threat intelligence program. This can result in "noise," which refers to irrelevant or false information that can distract from real threats, and potentially put the organization's network at risk. Verifying the credibility and reliability of intelligence sources is crucial to ensure that the data used for making security decisions is accurate and actionable.References:
* "Best Practices for Threat Intelligence Sharing," by FIRST (Forum of Incident Response and Security Teams)
* "Evaluating Cyber Threat Intelligence Sources," by Jon DiMaggio, SANS Institute InfoSec Reading
* Room

NEW QUESTION # 62
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.

- A. Conducting a gap analysis
- B. Determining the fulfillment of stakeholders

- C. Determining the costs and benefits associated with the program
- D. Identifying areas of further improvement

Answer: A

Explanation:
By assessing the Threat Intelligence (TI) program through a comparison of project results with the original objectives, and by ensuring that all expected deliverables have been produced to an acceptable quality level, Joe is conducting a gap analysis. Gap analysis involves identifying the difference between the current state and the desired state or objectives, in this case, the outcomes of the TI program versus its intended goals as outlined in the project charter. This process allows for the assessment of what was successful, what fell short, and where improvements can be made, thereby evaluating the program's overall effectiveness and identifying areas for future enhancement.
References:
"Project Management Body of Knowledge (PMBOK)" by the Project Management Institute
"Intelligence Analysis: A Target-Centric Approach" by Robert M. Clark

NEW QUESTION # 63
.....