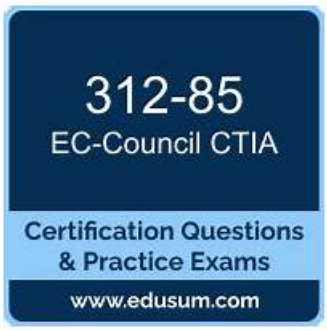
312-85 Exam Vce & 312-85 Valid Exam Papers



BTW, DOWNLOAD part of TestBraindump 312-85 dumps from Cloud Storage: https://drive.google.com/open?id=1nC8SRoyEUzlmTNnhT8DII7fPh_p9Xrpi

For some candidates who will attend the exam, they may have the concern that they can't pass the exam. 312-85 study guide have the questions and answers for you to train, and we will be pass guaranteed and money back guaranteed, that is to say, if you can't pass the exam, we will refund your money, or if you have another exam to attend, we will replace other 2 valid exam dumps for free, and if the 312-85 Exam Dumps updates, you can also get the free update for them. Choosing us, and you will benefit a lot.

To be eligible to take the exam, candidates must have at least two years of experience in the field of cyber security, as well as a basic understanding of networking, security concepts, and operating systems. 312-85 exam consists of 100 multiple-choice questions, and candidates have two hours to complete it.

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 ECCouncil 312-85 Exam is designed for IT professionals who have at least two years of experience in the field of cybersecurity. Certified Threat Intelligence Analyst certification is vendor-neutral, which means that it is not tied to any specific technology or product. This makes the certification more valuable as it is recognized by all organizations, regardless of the technology they use. Certified Threat Intelligence Analyst certification is also ideal for those who are seeking to specialize in threat intelligence analysis and want to demonstrate their expertise in the field.

>> 312-85 Exam Vce <<

ECCouncil 312-85 Valid Exam Papers & Trustworthy 312-85 Source

In order to show you how efficient our 312-85 exam dump is, we allow you to download a demo version for free! You will have a chance to peak into the program and then make your final purchase decision. We are absolutely sure that once you see what's inside, you will buy it immediately without any hesitation! 312-85 Exam Dump also provide customer service, in case you have any inquiry or question, our professional Customer Support will be available for you 24/7. 365 days a Year.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q77-Q82):

NEW QUESTION # 77
Which of the following components refers to a node in the network that routes the traffic from a workstation to external command and control server and helps in identification of installed malware in the network?

- A. Hub
- B. Repeater
- C. Network interface card (NIC)
- D. Gateway

Answer: D

Explanation:
A gateway in a network functions as a node that routes traffic between different networks, such as from a local network to the internet. In the context of cyber threats, a gateway can be utilized to monitor and control the data flow to and from the network, helping in the identification and analysis of malware communications, including traffic to external command and control (C2) servers. This makes it an essential component in detecting installed malware within a network by observing anomalies or unauthorized communications at the network's boundary. Unlike repeaters, hubs, or network interface cards (NICs) that primarily facilitate network connectivity without analyzing the traffic, gateways can enforce security policies and detect suspicious activities.References:
* "Network Security Basics," Security+ Guide to Network Security Fundamentals
* "Malware Command and Control Channels: A Journey," SANS Institute InfoSec Reading Room

NEW QUESTION # 78
The cybersecurity team seeks to enhance its threat hunting capabilities in a large enterprise. They plan to search systematically and proactively for adversaries within their networks. What type of threat hunting approaches are they most likely to adopt, involving predefined processes, methodologies, and frameworks for their investigation?

- A. Structured threat hunting
- B. Unstructured threat hunting
- C. Situational threat hunting
- D. Entity-driven threat hunting

Answer: A

Explanation:
Structured Threat Hunting uses predefined methodologies, frameworks, and processes to conduct proactive searches for adversaries within networks.
This approach relies on:
* Established frameworks like MITRE ATT&CK or Diamond Model.
* Standardized investigation workflows.
* Defined hypotheses and repeatable steps for analysis.
It ensures consistency and repeatability in the organization's hunting efforts.
Why the Other Options Are Incorrect:
* A. Situational threat hunting: Focuses on specific incidents or triggers rather than predefined methodologies.
* C. Entity-driven threat hunting: Centers on specific users, hosts, or IP addresses based on observed indicators.
* D. Unstructured threat hunting: Ad-hoc and experience-driven, lacking standardized methods.
Conclusion:
The team is using Structured Threat Hunting, which employs standardized frameworks and processes.
Final Answer: B. Structured threat hunting
Explanation Reference (Based on CTIA Study Concepts):
Structured hunting is described in CTIA as a systematic, framework-based approach that uses defined methodologies for consistent and effective investigations.

NEW QUESTION # 79
Two cybersecurity teams from different organizations joined forces to combat a rapidly evolving malware campaign targeting their

industry. They exchange real-time information about the attackers' techniques, compromised systems, and immediate defensive actions. What type of threat intelligence sharing characterizes this collaboration?

- A. Sharing strategic threat intelligence
- B. Sharing tactical threat intelligence
- C. Sharing operational threat intelligence
- D. Sharing technical threat intelligence

Answer: B

Explanation:
The exchange of attack techniques, compromised systems, and immediate defensive actions represents Tactical Threat Intelligence sharing.
Tactical Threat Intelligence focuses on adversary Tactics, Techniques, and Procedures (TTPs) and helps defenders understand and counter ongoing attacks in real time.
Why the Other Options Are Incorrect:
* B. Operational: Focuses on broader attack campaigns and contextual analysis.
* C. Strategic: Provides high-level, long-term insights for executives.
* D. Technical: Concerns low-level indicators like IPs and file hashes, not methodologies or immediate actions.
Conclusion:
The collaboration involves Tactical Threat Intelligence, which centers on sharing actionable TTPs and response techniques.
Final Answer: A. Sharing tactical threat intelligence
Explanation Reference (Based on CTIA Study Concepts):
CTIA defines tactical threat intelligence as intelligence describing attacker behaviors and techniques that can be acted upon immediately by defenders.

NEW QUESTION # 80
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. Refinement
- B. Diagnostics
- C. Inconsistency
- D. Evidence

Answer: A

Explanation:
In the Analysis of Competing Hypotheses (ACH) process, the stage where Mr. Bob is applying analysis to reject hypotheses and select the most likely one based on listed evidence, followed by preparing a matrix with screened hypotheses and evidence, is known as the 'Refinement' stage. This stage involves refining the list of hypotheses by systematically evaluating the evidence against each hypothesis, leading to the rejection of inconsistent hypotheses and the strengthening of the most plausible ones. The preparation of a matrix helps visualize the relationship between each hypothesis and the available evidence, facilitating a more objective and structured analysis.References:
* "Psychology of Intelligence Analysis" by Richards J. Heuer, Jr., for the CIA's Center for the Study of Intelligence
* "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis" by the CIA

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. True attribution
- C. Campaign attribution
- D. Nation-state attribution

Answer: B

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
.....

After clients pay successfully for our Certified Threat Intelligence Analyst guide torrent, they will receive our mails sent by our system in 5-10 minutes. Then they can dick the mail and log in to use our software to learn immediately. For that time is extremely important for the learners, everybody hope that they can get the efficient learning. So clients can use our 312-85 test torrent immediately is the great merit of our product. We have set strict computer procedure to protect the client's privacy about purchasing 312-85 Study Tool and there is no one which can see the privacy information through online or other illegal channels except us. We have set the rigorous interception procedure to protect others from stealing the client's personal privacy information.