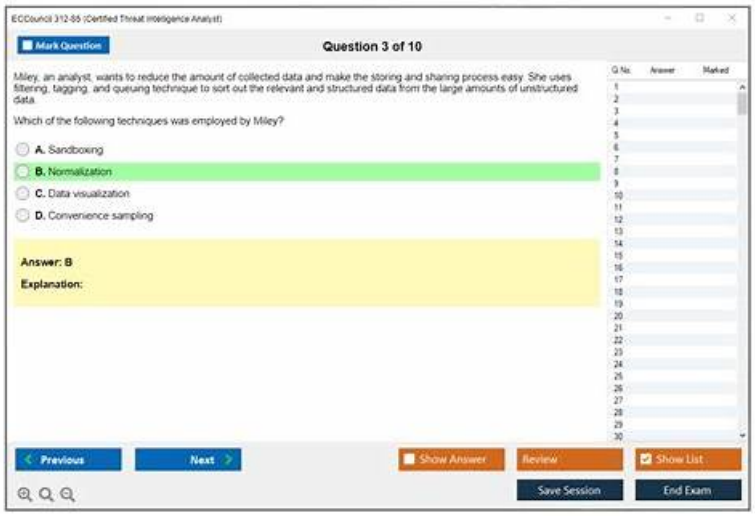
Boost Your Preparation with DumpStillValid ECCouncil 312-85 Online Practice Test Software



What's more, part of that DumpStillValid 312-85 dumps now are free: https://drive.google.com/open?id=1cfFMNWaPY6NJz4FyDO7Qyh1HRMdafsJd

Every practice exam or virtual exam of the 312-85 study materials is important for you. It is a good chance to test your current revision conditions. So it is essential to summarize each exercise to help you adjust your review plan. Now, we have added a new function to our online test engine and windows software of the 312-85 Real Exam, which can automatically generate a report according to your exercises of the 312-85 exam questions.

To prepare for the ECCouncil 312-85 exam, candidates are advised to take a comprehensive training course that covers all the topics that will be covered on the exam. Candidates should also have hands-on experience in threat intelligence, and be familiar with the latest tools and techniques used in the industry. 312-85 Exam is a rigorous test of the candidate's knowledge and skills, and passing the exam is a significant achievement that demonstrates the candidate's expertise in threat intelligence.

>> 312-85 Free Sample Questions <<

ECCouncil 312-85 Valid Test Cram | 312-85 Guide Torrent

Before you decide to get the 312-85 exam certification, you may be attracted by the benefits of 312-85 credentials. Get certified by 312-85 certification means you have strong professional ability to deal with troubleshooting in the application. Besides, you will get promotion in your job career and obtain a higher salary. If you want to pass your ECCouncil 312-85 Actual Test at first attempt, 312-85 pdf torrent is your best choice. The high pass rate of 312-85 vce dumps can give you surprise.

ECCouncil 312-85 Exam covers a wide range of topics, including threat intelligence fundamentals, cyber threat intelligence frameworks, threat modeling, attack vectors and malware analysis, incident response, and threat detection techniques. 312-85 exam also focuses on the practical application of threat intelligence analysis, evaluating how well the candidate can apply the concepts learned in real-world scenarios. 312-85 Exam is intended for professionals who have a minimum of two years of experience in the information security domain and are looking to advance their career.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q72-Q77):

NEW QUESTION # 72
Kim, an analyst, is looking for an intelligence-sharing platform to gather and share threat information from a variety of sources. He wants to use this information to develop security policies to enhance the overall security posture of his organization.
Which of the following sharing platforms should be used by Kim?

- A. OmniPeek

- B. Cuckoo sandbox
- C. PortDroid network analysis
- D. Blueliv threat exchange network

Answer: D

Explanation:
The Blueliv Threat Exchange Network is a collaborative platform designed for sharing and receiving threat intelligence among security professionals and organizations. It provides real-time information on global threats, helping participants to enhance their security posture by leveraging shared intelligence. The platform facilitates the exchange ofinformation related to cybersecurity threats, including indicators of compromise (IoCs), tactics, techniques, and procedures (TTPs) of threat actors, and other relevant data. This makes it an ideal choice for Kim, who is looking to gather and share threat information to develop security policies for his organization. In contrast, Cuckoo Sandbox is a malware analysis system, OmniPeek is a network analyzer, and PortDroid is a network analysis application, none of which are primarily designed for intelligence sharing.References:
* Blueliv's official documentation and resources
* "Building an Intelligence-Led Security Program," by Allan Liska

NEW QUESTION # 73
Daniel is a professional hacker whose aim is to attack a system to steal data and money for profit. He performs hacking to obtain confidential data such as social security numbers, personally identifiable information (PII) of an employee, and credit card information. After obtaining confidential data, he further sells the information on the black market to make money.
Daniel comes under which of the following types of threat actor.

- A. Organized hackers
- B. Insider threat
- C. Industrial spies
- D. State-sponsored hackers

Answer: A

NEW QUESTION # 74
Michael, a threat analyst, works in an organization named TechTop, was asked to conduct a cyber-threat intelligence analysis. After obtaining information regarding threats, he has started analyzing the information and understanding the nature of the threats.
What stage of the cyber-threat intelligence is Michael currently in?

- A. Known knowns
- B. Unknowns unknown
- C. Known unknowns
- D. Unknown unknowns

Answer: C

NEW QUESTION # 75
Jim works as a security analyst in a large multinational company. Recently, a group of hackers penetrated into their organizational network and used a data staging technique to collect sensitive data. They collected all sorts of sensitive data about the employees and customers, business tactics of the organization, financial information, network infrastructure information and so on.
What should Jim do to detect the data staging before the hackers exfiltrate from the network?

- A. Jim should monitor network traffic for malicious file transfers, file integrity monitoring, and event logs.
- B. Jim should identify the web shell running in the network by analyzing server access, error logs, suspicious strings indicating encoding, user agent strings, and so on.
- C. Jim should analyze malicious DNS requests, DNS payload, unspecified domains, and destination of DNS requests.
- D. Jim should identify the attack at an initial stage by checking the content of the user agent field.

Answer: A

Explanation:
In the scenario described, where attackers have penetrated the network and are staging data for exfiltration, Jim should focus on

monitoring network traffic for signs of malicious file transfers, implement file integrity monitoring, and scrutinize event logs. This approach is crucial for detecting unusual activity that could indicate data staging, such as large volumes of data being moved to uncommon locations, sudden changes in file integrity, or suspicious entries in event logs. Early detection of these indicators can help in identifying the staging activity before the data is exfiltrated from the network.References:
* NIST Special Publication 800-61 Rev. 2, "Computer Security Incident Handling Guide"
* SANS Institute Reading Room, "Detecting Malicious Activity with DNS and NetFlow"

NEW QUESTION # 76
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 technical threat intelligence
- C. Sharing operational threat intelligence
- D. Sharing tactical threat intelligence

Answer: D

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 # 77
.....

- 312-85 Valid Braindumps Sheet Reliable 312-85 Exam Bootcamp 312-85 Valid Exam Cost Easily obtain ✔ 312-85 ✔ for free download through 【 www.pdfvce.com 】 312-85 Valid Braindumps Sheet
- Free Download 312-85 Free Sample Questions - High-quality 312-85 Valid Test Cram Ensure You a High Passing Rate   Search for 312-85 and download it for free immediately on ➥ www.pass4test.com Free 312-85 Dumps
- 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.sxrsedu.cn, 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.du71l.cn, 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, pianowithknight.com, Disposable vapes

P.S. Free 2026 ECCouncil 312-85 dumps are available on Google Drive shared by DumpStillValid: https://drive.google.com/open?id=1cfFMNWaPY6NJz4FyDO7Qyh1HRMdafsJd