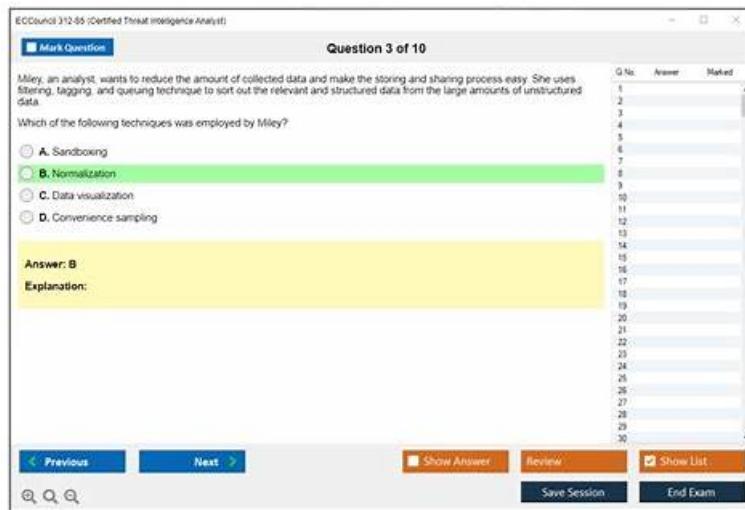


Web-based ECCouncil 312-85 Practice Exam Software - Solution for Online Self-Assessment



What's more, part of that PassTestking 312-85 dumps now are free: https://drive.google.com/open?id=1OBGVa5R-SYeBtH97tqaRBxs2Fhq_aYG9

In order to meet the demands of all customers, our company has a complete set of design, production and service quality guarantee system, the 312-85 study materials are perfect. We can promise that quality first, service upmost. If you buy the 312-85 study materials from our company, we are glad to provide you with the high quality 312-85 Study Materials and the best service. The philosophy of our company is "quality is life, customer is god." We can promise that our company will provide all customers with the perfect quality guarantee system and sound management system.

The CTIA certification exam (312-85) consists of 100 multiple-choice questions that must be completed in a time frame of three hours. 312-85 exam covers four domains: Introduction to Threat Intelligence, Requirements Gathering for Threat Intelligence, Threat Intelligence Analysis Techniques, and Threat Intelligence Application. 312-85 exam is designed to test candidates' knowledge and skills in threat intelligence analysis, including the ability to identify and analyze threats, develop intelligence reports, and implement threat intelligence programs effectively.

The Certified Threat Intelligence Analyst exam covers various topics that are essential in the field of cybersecurity. 312-85 Exam focuses on identifying and analyzing different types of cyber threats, understanding the tactics used by attackers, and applying the appropriate countermeasures to mitigate the risks. 312-85 exam also covers the latest trends in threat intelligence analysis, including the use of artificial intelligence and machine learning techniques.

[**>> Exam 312-85 Questions Fee <<**](#)

Latest updated Exam 312-85 Questions Fee | Easy To Study and Pass Exam at first attempt & Hot ECCouncil Certified Threat Intelligence Analyst

Now there are many IT training institutions which can provide you with ECCouncil certification 312-85 exam related training material, but usually through these website examinees do not gain detailed material. Because the materials they provide are specialized for ECCouncil Certification 312-85 Exam, so they didn't attract the examinee's attention.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q43-Q48):

NEW QUESTION # 43

Alice, a threat intelligence analyst at HiTech Cyber Solutions, wants to gather information for identifying emerging threats to the organization and implement essential techniques to prevent their systems and networks from such attacks. Alice is searching for online sources to obtain information such as the method used to launch an attack, and techniques and tools used to perform an

attack and the procedures followed for covering the tracks after an attack.
Which of the following online sources should Alice use to gather such information?

- A. Financial services
- B. Social network settings
- C. Hacking forums
- D. Job sites

Answer: C

Explanation:

Alice, looking to gather information on emerging threats including attack methods, tools, and post-attack techniques, should turn to hacking forums. These online platforms are frequented by cybercriminals and security researchers alike, where information on the latest exploits, malware, and hacking techniques is shared and discussed. Hacking forums can provide real-time insights into the tactics, techniques, and procedures (TTPs) used by threat actors, offering a valuable resource for threat intelligence analysts aiming to enhance their organization's defenses. References:

* "Hacking Forums: A Ground for Cyber Threat Intelligence," by Digital Shadows

* "The Value of Hacking Forums for Threat Intelligence," by Flashpoint

NEW QUESTION # 44

Lizzy, an analyst, wants to recognize the level of risks to the organization so as to plan countermeasures against cyber attacks. She used a threat modelling methodology where she performed the following stages:

Stage 1: Build asset-based threat profiles

Stage 2: Identify infrastructure vulnerabilities

Stage 3: Develop security strategy and plans

Which of the following threat modelling methodologies was used by Lizzy in the aforementioned scenario?

- A. OCTAVE
- B. VAST
- C. DREAD
- D. TRIKE

Answer: A

Explanation:

The threat modeling methodology employed by Lizzy, which involves building asset-based threat profiles, identifying infrastructure vulnerabilities, and developing security strategies and plans, aligns with the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) methodology. OCTAVE focuses on organizational risk and security practices, emphasizing self-directed risk assessments to identify and prioritize threats to organizational assets and develop appropriate security strategies and plans. This methodology is asset-driven and revolves around understanding critical assets, identifying threats to those assets, and assessing vulnerabilities, leading to the development of a comprehensive security strategy. References:

* The CERT Guide to System and Network Security Practices by Julia H. Allen

* "OCTAVE Method Implementation Guide Version 2.0," Carnegie Mellon University, Software Engineering Institute

NEW QUESTION # 45

Alison, an analyst in an XYZ organization, wants to retrieve information about a company's website from the time of its inception as well as the removed information from the target website.

What should Alison do to get the information he needs.

- A. Alison should use SmartWhois to extract the required website information.
- B. Alison should use <https://archive.org> to extract the required website information.
- C. Alison should recover cached pages of the website from the Google search engine cache to extract the required website information.
- D. Alison should run the Web Data Extractor tool to extract the required website information.

Answer: D

NEW QUESTION # 46

Tyrion, a professional hacker, is targeting an organization to steal confidential information. He wants to perform website footprinting to obtain the following information, which is hidden in the web page header.

Connection status and content type

Accept-ranges and last-modified information

X-powered-by information

Web server in use and its version

Which of the following tools should the Tyrion use to view header content?

- A. Vanguard enforcer
- B. AutoShun
- C. Hydra
- D. **Burp suite**

Answer: D

NEW QUESTION # 47

Alice, an analyst, shared information with security operation managers and network operations center (NOC) staff for protecting the organizational resources against various threats. Information shared by Alice was highly technical and include threat actor TTPs, malware campaigns, tools used by threat actors, and so on.

Which of the following types of threat intelligence was shared by Alice?

- A. Strategic threat intelligence
- B. **Tactical threat intelligence**
- C. Operational threat intelligence
- D. Technical threat intelligence

Answer: B

Explanation:

The information shared by Alice, which was highly technical and included details such as threat actor tactics, techniques, and procedures (TTPs), malware campaigns, and tools used by threat actors, aligns with the definition of tactical threat intelligence. This type of intelligence focuses on the immediate, technical indicators of threats and is used by security operation managers and network operations center (NOC) staff to protect organizational resources. Tactical threat intelligence is crucial for configuring security solutions and adjusting defense mechanisms to counteract known threats effectively.

References:

"Tactical Cyber Intelligence," Cyber Threat Intelligence Network, Inc.

"Cyber Threat Intelligence for Front Line Defenders: A Practical Guide," by James Dietle

NEW QUESTION # 48

.....

We should formulate a set of high efficient study plan to make the 312-85 exam dumps easier to operate. Here our products strive for providing you a comfortable study platform and continuously upgrade 312-85 test prep to meet every customer's requirements. Under the guidance of our 312-85 Test Braindumps, 20-30 hours' preparation is enough to help you obtain the ECCouncil certification, which means you can have more time to do your own business as well as keep a balance between a rest and taking exams.

312-85 Reliable Braindumps: <https://www.passtestking.com/ECCouncil/312-85-practice-exam-dumps.html>

- Achieve an Excellent Score in Your ECCouncil 312-85 Exam with www.validtorrent.com Enter ➤ www.validtorrent.com and search for ➡ 312-85 to download for free 312-85 Reliable Braindumps
- 312-85 Best Study Material New Soft 312-85 Simulations 312-85 Reliable Real Exam Immediately open ✓ www.pdfvce.com ✓ and search for 《 312-85 》 to obtain a free download Real 312-85 Exam Dumps
- 312-85 Test Lab Questions 312-85 Valid Dump Valid 312-85 Dumps Copy URL (www.prep4away.com) open and search for ➡ 312-85 to download for free Exam 312-85 Exercise
- 100% Pass Quiz Useful ECCouncil - 312-85 - Exam Certified Threat Intelligence Analyst Questions Fee Go to website www.pdfvce.com www.pdfvce.com open and search for " 312-85 " to download for free 312-85 Training Courses
- 2026 ECCouncil Exam 312-85 Questions Fee - Certified Threat Intelligence Analyst Realistic Reliable Braindumps 100% Pass The page for free download of [312-85](http://www.dumpsquestion.com) www.dumpsquestion.com on www.dumpsquestion.com will open immediately

□312-85 Free Exam Dumps

P.S. Free & New 312-85 dumps are available on Google Drive shared by PassTestking: https://drive.google.com/open?id=1OBGVa5R-SYEcBtH97tqaRBxs2Fhq_aYG9