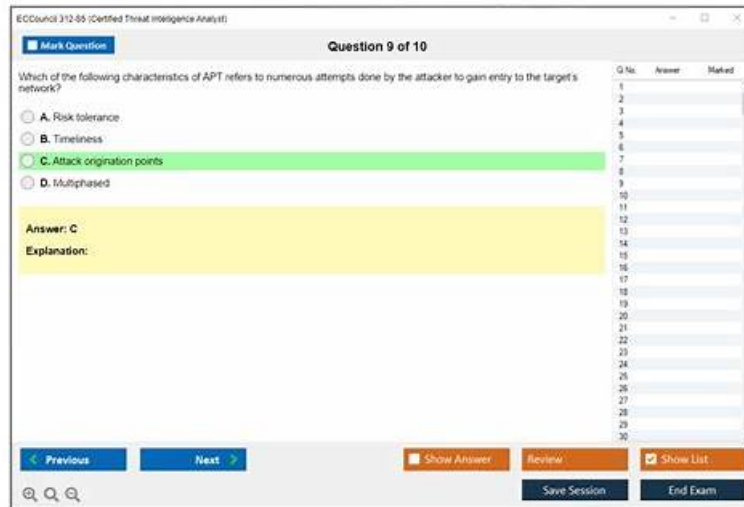


Start Your Journey to Success with TestKingFree ECCouncil 312-85 Practice Material



P.S. Free & New 312-85 dumps are available on Google Drive shared by TestKingFree: https://drive.google.com/open?id=12rXmzbVgUQZVb1_TqwTGFbgmj3eySG4

The ECCouncil 312-85 certification provides is beneficial to accelerate your career in the tech sector. Today, the 312-85 is a fantastic choice to get high-paying jobs and promotions, and to achieve it, you must crack the challenging ECCouncil exam. It is critical to prepare with actual 312-85 Exam Questions if you have less time and want to clear the test in a short time. You will fail and waste time and money if you do not prepare with real and updated ECCouncil 312-85 Questions.

By offering the most considerate after-sales services of 312-85 exam torrent materials for you, our whole package services have become famous and if you hold any questions after buying Certified Threat Intelligence Analyst prepare torrent, get contact with our staff at any time, they will solve your problems with enthusiasm and patience. They do not shirk their responsibility of offering help about 312-85 Test Braindumps for you 24/7 that are wary and considerate for every exam candidate's perspective. Understanding and mutual benefits are the cordial principles of services industry. We know that tenet from the bottom of our heart, so all parts of service are made due to your interests.

>> Exam 312-85 Answers <<

Top Features of TestKingFree 312-85 Certified Threat Intelligence Analyst PDF Questions File and Practice Test Software

Improvement in 312-85 science and technology creates unassailable power in the future construction and progress of society. As we can see, the rapid progression of the whole world is pushing people forward and the competitiveness among people who are fighting on the first line is growing intensely. Numerous advantages of 312-85 training materials are well-recognized, such as 99% pass rate in the exam, free trial before purchasing, secure privacy protection and so forth. From the customers' point of view, our 312-85 Test Question put all candidates' demands as the top priority. We treasure every customer' reliance and feedback to the optimal 312-85 practice test.

The Certified Threat Intelligence Analyst certification exam covers a range of topics including the fundamentals of cybersecurity threats, the principles of threat intelligence, the use of threat intelligence tools and techniques, and the legal and ethical issues surrounding the use of threat intelligence. 312-85 exam is designed to test the candidate's ability to apply their knowledge in real-world scenarios and to identify and respond to cyber threats effectively.

ECCouncil 312-85 exam, also known as the Certified Threat Intelligence Analyst (CTIA) exam, is a certification exam designed for professionals who want to demonstrate their knowledge and skills in threat intelligence analysis. 312-85 Exam is designed to test the candidate's ability to collect, analyze, and interpret threat intelligence data to identify potential security threats and vulnerabilities. 312-85 exam covers a wide range of topics, including threat intelligence frameworks, tools, techniques, and best practices.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q81-Q86):

NEW QUESTION # 81

You are a Security Operations Center (SOC) analyst responsible for monitoring and safeguarding the organization's network. During routine activities, you identify a potential vulnerability that can expose critical systems to exploitation. In what specific aspect of cybersecurity would you actively engage in when addressing and mitigating this vulnerability?

- A. Incident response
- **B. Vulnerability management**
- C. Threat intelligence analysis
- D. Security awareness training

Answer: B

Explanation:

The process of identifying, assessing, and mitigating vulnerabilities in systems is part of Vulnerability Management.

Vulnerability Management involves:

- * Detecting potential weaknesses or misconfigurations.
- * Assessing their severity and prioritizing fixes.
- * Applying patches or other mitigation controls.
- * Verifying that remediation efforts are successful.

While threat intelligence provides contextual data, the actual handling and resolution of discovered vulnerabilities fall under vulnerability management.

Why the Other Options Are Incorrect:

- * A. Threat intelligence analysis: Focuses on gathering and analyzing threat data, not fixing vulnerabilities.
- * C. Security awareness training: Involves educating staff, not mitigating technical issues.
- * D. Incident response: Comes into play after an incident has occurred; this scenario focuses on prevention.

Conclusion:

The analyst is engaged in Vulnerability Management, aimed at reducing the risk of exploitation before an attack occurs.

Final Answer: B. Vulnerability management

Explanation Reference (Based on CTIA Study Concepts):

Vulnerability management is emphasized as a preventive cybersecurity function that identifies and mitigates exploitable weaknesses.

NEW QUESTION # 82

Moses, a threat intelligence analyst at InfoTec Inc., wants to find crucial information about the potential threats the organization is facing by using advanced Google search operators. He wants to identify whether any fake websites are hosted at the similar to the organization's URL.

Which of the following Google search queries should Moses use?

- A. cache: www.infotech.org
- **B. related: www.infotech.org**
- C. link: www.infotech.org
- D. info: www.infotech.org

Answer: B

Explanation:

The "related:" Google search operator is used to find websites that are similar or related to a specified URL.

In the context provided, Moses wants to identify fake websites that may be posing as or are similar to his organization's official site. By using the "related:" operator followed by his organization's URL, Google will return a list of websites that Google considers to be similar to the specified site. This can help Moses identify potential impersonating websites that could be used for phishing or other malicious activities. The "info:",

"link:", and "cache:" operators serve different purposes; "info:" provides information about the specified webpage, "link:" used to be used to find pages linking to a specific URL (but is now deprecated), and "cache:" shows the cached version of the specified webpage.

References:

Google Search Operators Guide by Moz

Google Advanced Search Help Documentation

NEW QUESTION # 83

An XYZ organization hired Mr. Andrews, a threat analyst. In order to identify the threats and mitigate the effect of such threats, Mr. Andrews was asked to perform threat modeling. During the process of threat modeling, he collected important information about the threat actor and characterized the analytic behavior of the adversary that includes technological details, goals, and motives that can be useful in building a strong countermeasure.

What stage of the threat modeling is Mr. Andrews currently in?

- A. Threat determination and identification
- B. System modeling
- C. Threat ranking
- **D. Threat profiling and attribution**

Answer: D

Explanation:

During the threat modeling process, Mr. Andrews is in the stage of threat profiling and attribution, where he is collecting important information about the threat actor and characterizing the analytic behavior of the adversary. This stage involves understanding the technological details, goals, motives, and potential capabilities of the adversaries, which is essential for building effective countermeasures. Threat profiling and attribution help in creating a detailed picture of the adversary, contributing to a more focused and effective defense strategy.

References:

* "The Art of Threat Profiling," by John Pirc, SANS Institute Reading Room

* "Threat Modeling: Designing for Security," by Adam Shostack

NEW QUESTION # 84

Cybersol Technologies initiated a cyber-threat intelligence program with a team of threat intelligence analysts.

During the process, the analysts started converting the raw data into useful information by applying various techniques, such as machine-based techniques, and statistical methods.

In which of the following phases of the threat intelligence lifecycle is the threat intelligence team currently working?

- A. Dissemination and integration
- **B. Processing and exploitation**
- C. Planning and direction
- D. Analysis and production

Answer: B

Explanation:

The phase where threat intelligence analysts convert raw data into useful information by applying various techniques, such as machine learning or statistical methods, is known as 'Processing and Exploitation'. During this phase, collected data is processed, standardized, and analyzed to extract relevant information. This is a critical step in the threat intelligence lifecycle, transforming raw data into a format that can be further analyzed and turned into actionable intelligence in the subsequent 'Analysis and Production' phase.

References:

* "Intelligence Analysis for Problem Solvers" by John E. McLaughlin

* "The Cyber Intelligence Tradecraft Project: The State of Cyber Intelligence Practices in the United States (Unclassified Summary)" by the Carnegie Mellon University's Software Engineering Institute

NEW QUESTION # 85

In which of the following storage architecture is the data stored in a localized system, server, or storage hardware and capable of storing a limited amount of data in its database and locally available for data usage?

- **A. Centralized storage**
- B. Cloud storage
- C. Object-based storage
- D. Distributed storage

Answer: A

Explanation:

- * "Data Storage Solutions for Your Business: Centralized vs. Decentralized," Techopedia
- * "The Basics of Centralized Data Storage," by Margaret Rouse, SearchStorage

• • • • •

312-85 VCE Exam Simulator: <https://www.testkingfree.com/ECCouncil/312-85-practice-exam-dumps.html>

- BONUS!!! Download part of TestKingFree 312-85 dumps for free: <https://drive.google.com/open?id=12rXmzbVgUOZVb1TqwTGFbgmzi3evSG4>