Valid 312-85 Test Objectives & 312-85 Free Practice Exams


ECCouncil 312-85 Certified Threat Intelligence Analyst 4

Dumps 312-85 Zip

- 100% Pass Quiz 2023 ECCouncil 312-85: Certified Threat Intelligence Analyst - High Pass-Rate Simulations Pdf □ Search for □ 312-85 □ and obtain a free download on □ www.pdfvce.com □ □Latest 312-85 Exam Papers
- Free PDF 2023 Trustable ECCouncil 312-85: Simulations Certified Threat Intelligence Analyst Pdf □ Simply search for " 312-85 " for free download on ▶ www.pdfvce.com ◀ □312-85 Reliable Exam Review
- Exam Dumps 312-85 Zip □ Minimum 312-85 Pass Score □ 312-85 Training Online □ □ www.pdfvce.com □ is best website to obtain ▷ 312-85 ◁ for free download □312-85 Valid Exam Registration
- 312-85 Reliable Exam Review ⏏ 312-85 Reliable Exam Review □ 312-85 Relevant Answers □ Open □ www.pdfvce.com □ enter " 312-85 " and obtain a free download □312-85 New Real Test
- 2023 Simulations 312-85 Pdf - ECCouncil Certified Threat Intelligence Analyst - Trustable Actual 312-85 Test □ ▶ www.pdfvce.com ◀ is best website to obtain ➡ 312-85 ⬅ for free download □312-85 Latest Test Guide
- Latest 312-85 Study Notes □ 312-85 Relevant Answers □ 312-85 Online Test □ Easily obtain ▷ 312-85 ◁ for free download through ➡ www.pdfvce.com ⬅ ▶Exam Dumps 312-85 Zip

Tags: **Simulations 312-85 Pdf,Actual 312-85 Test,312-85 Premium Files,312-85 Questions Pdf,312-85 Dumps Reviews**

HOT Simulations 312-85 Pdf - High Pass-Rate ECCouncil Actual 312-85 Test: Certified Threat Intelligence Analyst

BTW, DOWNLOAD part of Free4Torrent 312-85 dumps from Cloud Storage: https://drive.google.com/open?id=1EaQK5YTtFqI7dzpXgz0JaMxXJ58_KgcD

The pass rate is 98.75% for 312-85 study materials, and if you choose us, we can ensure you that you can pass the exam just one time. 312-85 exam dumps are high-quality and high accuracy, since we have a professional team to compile and examine the questions and answers. What's more, 312-85 exam materials have both questions and answers, and you can check your answers very conveniently after practicing. We offer you free update for one year for 312-85 Study Materials, and our system will send the latest version to your email address automatically, and you need to receive and change your learning ways according to the latest version.

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.

>> Valid 312-85 Test Objectives <<

You Can Never Think About Failure With ECCouncil 312-85 Exam Dumps

If you want to strive for a further improvement in the IT industry, it's right to choose our Free4Torrent. Free4Torrent's 312-85 exam certification training materials is worked out by IT industry elite team through their own exploration and continuous practice. It has high accuracy and wide coverage. Owning Free4Torrent's 312-85 Exam Certification training materials is equal to have the key to success.

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

NEW QUESTION # 77
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. Blueliv threat exchange network
- B. OmniPeek
- C. Cuckoo sandbox
- D. PortDroid network analysis

Answer: A

NEW QUESTION # 78
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. State-sponsored hackers
- B. Insider threat
- C. Organized hackers
- D. Industrial spies

Answer: C

Explanation:
Daniel's activities align with those typically associated with organized hackers. Organized hackers or cybercriminals work in groups with the primary goal of financial gain through illegal activities such as stealing and selling data. These groups often target large amounts of data, including personal and financial information, which they can monetize by selling on the black market or dark web. Unlike industrial spies who focuson corporate espionage or state-sponsored hackers who are backed by nation-states for political or military objectives, organized hackers are motivated by profit. Insider threats, on the other hand, come from within the organization and might not always be motivated by financial gain. The actions described in the scenario-targeting personal and financial information for sale-best fit the modus operandi of organized cybercriminal groups.References:
* ENISA (European Union Agency for Cybersecurity) Threat Landscape Report
* Verizon Data Breach Investigations Report

NEW QUESTION # 79
To extract useful intelligence from the gathered bulk data and to improve the efficiency of the composite bulk data, Sam, a threat analyst, follows a data analysis method where he creates a logical sequence of events based on the assumptions of an adversary's proposed actions, mechanisms, indicators, and implications. To develop accurate predictions, he further takes into consideration the important factors including bad actors, methods, vulnerabilities, targets, and so on.
Which of the following data analysis methods is used by Sam to extract useful intelligence out of bulk data?

- A. Analogy analysis
- B. Opportunity analysis
- C. Linchpin analysis
- D. Critical path analysis

Answer: D

Explanation:

The description provided in the question directly matches the concept of Critical Path Analysis (CPA) as used in threat intelligence analysis.
In CTIA, Critical Path Analysis is a structured analytical technique used to determine the logical sequence of adversarial actions or events that could lead to a specific outcome. It helps analysts create a timeline or chain of likely activities based on adversary behavior, available vulnerabilities, and possible targets.
This method involves constructing a logical flow of actions that an attacker might take - such as reconnaissance, exploitation, lateral movement, and data exfiltration - and identifying key points in that chain where defenders can detect or disrupt the attack.
Key Characteristics of Critical Path Analysis:
* It helps identify cause-and-effect relationships between adversarial actions.
* It is assumption-driven, based on observed patterns, indicators, and adversary intent.
* It allows prediction of future attacker behavior by modeling their likely paths and objectives.
* It supports prioritization of defensive measures at critical stages of an attack.
Why the Other Options Are Incorrect:
* B. Linchpin analysis:Focuses on identifying the key individual, node, or factor that plays a pivotal role in an adversary's operation. It is used for identifying the "weakest link" to disrupt the threat actor's network, not for sequencing adversary actions.
* C. Analogy analysis:Involves comparing current situations or attack patterns with previous known cases to infer potential behaviors or outcomes. It relies on historical similarities, not on logical event sequencing.
* D. Opportunity analysis:Focuses on identifying areas where intelligence can create opportunities to mitigate or exploit a situation. It's used for strategic planning, not constructing adversarial timelines.
Conclusion:
Sam used Critical Path Analysis to model the attacker's likely actions and derive meaningful intelligence from large volumes of data.
Final Answer: A. Critical Path Analysis
Explanation Reference (Based on CTIA Study Concepts):
As per CTIA analysis techniques, Critical Path Analysis is used for building logical sequences of adversarial events to anticipate attacker behavior and improve prediction accuracy.

NEW QUESTION # 80
In which of the following forms of bulk data collection are large amounts of data first collected from multiple sources in multiple formats and then processed to achieve threat intelligence?

- A. Structured form
- B. Unstructured form
- C. Production form
- D. Hybrid form

Answer: B

Explanation:
In the context of bulk data collection for threat intelligence, data is often initially collected in an unstructured form from multiple sources and in various formats. This unstructured data includes information from blogs, news articles, threat reports, social media, and other sources that do not follow a specific structure or format.
The subsequent processing of this data involves organizing, structuring, and analyzing it to extract actionable threat intelligence. This phase is crucial for turning vast amounts of disparate data into coherent, useful insights for cybersecurity purposes.
References:
"The Role of Unstructured Data in Cyber Threat Intelligence," by Jason Trost, Anomali
"Turning Unstructured Data into Cyber Threat Intelligence," by Giorgio Mosca, IEEE Xplore

NEW QUESTION # 81
Jian is a member of the security team at Trinity, Inc. He was conducting a real-time assessment of system activities in order to acquire threat intelligence feeds. He acquired feeds from sources like honeynets, P2P monitoring. infrastructure, and application logs.
Which of the following categories of threat intelligence feed was acquired by Jian?

- A. Internal intelligence feeds
- B. CSV data feeds
- C. Proactive surveillance feeds
- D. External intelligence feeds

Answer: A

Explanation:
Internal intelligence feeds are derived from data and information collected within an organization's own networks and systems. Jian's activities, such as real-time assessment of system activities and acquiring feeds from honeynets, P2P monitoring, infrastructure, and application logs, fall under the collection of internal intelligence feeds. These feeds are crucial for identifying potential threats and vulnerabilities within the organization and form a fundamental part of a comprehensive threat intelligence program. They contrast with external intelligence feeds, which are sourced from outside the organization and include information on broader cyber threats, trends, and TTPs of threat actors.
References:
"Building an Intelligence-Led Security Program" by Allan Liska
"Threat Intelligence: Collecting, Analysing, Evaluating" by M-K. Lee, L. Healey, and P. A. Porras

NEW QUESTION # 82
.....