Pass Guaranteed Quiz ECCouncil - 312-85–High Pass-Rate Latest Braindumps Book


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

DOWNLOAD the newest DumpExam 312-85 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1zGNUZzoqr_4FHyYQeDmHrul1Ulo5QZ_Z

The ECCouncil 312-85 practice tests have customizable time and 312-85 exam questions feature so that the students can set the time and 312-85 exam questions according to their needs. The ECCouncil 312-85 practice test questions are getting updated on the daily basis and there are also up to 1 year of free updates. Earning the ECCouncil 312-85 Certification Exam is the way to grow in the modern era with high-paying jobs. The 24/7 support system is available for the customers so that they can get the solution to every problem they face and pass Certified Threat Intelligence Analyst (312-85) exam. You can also evaluate the 312-85 prep material with a free demo.

The CTIA certification exam is an excellent way for professionals to demonstrate their expertise in the field of threat intelligence analysis. Certified Threat Intelligence Analyst certification demonstrates that the candidate has a thorough understanding of the various aspects of threat intelligence analysis and is capable of identifying, assessing, and mitigating potential threats. Certified Threat Intelligence Analyst certification also shows that the candidate is committed to staying up-to-date with the latest developments in the field of cybersecurity and is dedicated to providing the best services to their clients.

>> Latest Braindumps 312-85 Book <<

312-85 Exam Simulator Online, 312-85 Well Prep

The objective of the DumpExam is to give you quick access to Certified Threat Intelligence Analyst (312-85) actual questions. Offering Certified Threat Intelligence Analyst (312-85) updated dumps is the only factor behind the dominance of DumpExam in the market. Our customers will see our Certified Threat Intelligence Analyst (312-85) questions in the final certification test. We have a devoted team who puts in a lot of effort to keep the 312-85 dumps updated. DumpExam informs you that the Certified Threat Intelligence Analyst (312-85) questions regularly change the content of the real exam.

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.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q89-Q94):

NEW QUESTION # 89
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. VAST
- B. TRIKE
- C. DREAD
- D. OCTAVE

Answer: D

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 # 90
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. Unknowns unknown
- B. Unknown unknowns
- C. Known knowns
- D. Known unknowns

Answer: D

NEW QUESTION # 91
An analyst is conducting threat intelligence analysis in a client organization, and during the information gathering process, he gathered information from the publicly available sources and analyzed to obtain a rich useful form of intelligence. The information source that he used is primarily used for national security, law enforcement, and for collecting intelligence required for business or strategic decision making.
Which of the following sources of intelligence did the analyst use to collect information?

- A. OSINT
- B. ISAC
- C. OPSEC
- D. SIGINT

Answer: A

Explanation:
The analyst used Open Source Intelligence (OSINT) to gather information from publicly available sources.
OSINT involves collecting and analyzing information from publicly accessible sources to produce actionable intelligence. This can include media reports, public government data, professional and academic publications, and information available on the internet. OSINT is widely used for national security, law enforcement, and business intelligence purposes, providing a rich source of information for making informed decisions and understanding the threat landscape.References:
* "Open Source Intelligence (OSINT) Tools and Techniques," by SANS Institute
* "The Role of OSINT in Cybersecurity and Threat Intelligence," by Recorded Future

NEW QUESTION # 92
You are a cybersecurity analyst working at a financial institution. An unusual pattern of financial transactions was detected, suggesting potential fraud or money laundering. What specific type of threat intelligence would you rely on to analyze these financial activities and identify potential risks?

- A. FININT
- B. OSINT
- C. CHIS
- D. TECHINT

Answer: A

Explanation:
FININT (Financial Intelligence) refers to the collection, processing, and analysis of financial transaction data to identify suspicious or illicit activities such as fraud, money laundering, terrorist financing, or financial crimes.
In this scenario, the analyst is investigating unusual financial transaction patterns, which is exactly the purpose of financial intelligence.
Key Features of FININT:
* Focuses on financial data sources, including transaction records, wire transfers, and account statements.
* Helps detect illicit financial flows or abnormal transaction behaviors.
* Used by banks, financial institutions, and government agencies to identify and prevent financial crimes.
* Often shared with intelligence agencies and regulatory bodies to support counter-fraud and anti-money laundering operations.
Why the Other Options Are Incorrect:
* A. OSINT:Refers to publicly available information such as websites, news, or social media. It is not specific to financial transaction data.
* B. CHIS:Refers to human intelligence sources obtained through personal or covert interaction, not financial data analysis.
* C. TECHINT:Refers to intelligence gathered from technical sources such as sensors or electronic systems, not financial records.
Conclusion:
The correct intelligence type used to analyze suspicious financial transactions is FININT (Financial Intelligence).
Final Answer: D. FININT
Explanation Reference (Based on CTIA Study Concepts):
As per CTIA threat intelligence classifications, FININT involves collecting and analyzing financial data to detect and mitigate fraudulent or criminal activities.

NEW QUESTION # 93
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 analyze malicious DNS requests, DNS payload, unspecified domains, and destination of DNS requests.
- B. Jim should monitor network traffic for malicious file transfers, file integrity monitoring, and event logs.
- C. 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.

- D. Jim should identify the attack at an initial stage by checking the content of the user agent field.

Answer: B

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 # 94
.....