Latest 312-85 Exam Topics, Exam 312-85 Overviews

What's more, part of that Itcertking 312-85 dumps now are free: https://drive.google.com/open?id=1OJHFQA0fAuiJLwaIRiOmzbxogAua3NwJ

In the major environment, people are facing more job pressure. So they want to get 312-85 certification rise above the common herd. How to choose valid and efficient 312-85 guide torrent should be the key topic most candidates may concern. So now, it is right, you come to us. Our company is famous for its high-quality in this field especially for 312-85 Certification exams. It has been accepted by thousands of candidates who practice our study materials for their exam.

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.

>> Latest 312-85 Exam Topics <<

Exam 312-85 Overviews & 312-85 Valid Exam Cram

With the help of Itcertking's marvelous brain dumps, you make sure your success in 312-85 certification exam with money back guarantee. Itcertking serves a huge network of its clientele with the state of the art and exam-oriented short-term study content that requires as little as a two-week time to get ready the entire 312-85 Certification syllabus.

The ECCouncil 312-85 Exam is designed for professionals who work in the field of cyber security, such as threat analysts, incident response personnel, and security operations center (SOC) analysts. It is also suitable for IT and network administrators who are responsible for managing an organization's security infrastructure.

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

NEW QUESTION # 77
Walter and Sons Company has faced major cyber attacks and lost confidential data. The company has decided to concentrate more on the security rather than other resources. Therefore, they hired Alice, a threat analyst, to perform data analysis. Alice was asked to perform qualitative data analysis to extract useful information from collected bulk data.
Which of the following techniques will help Alice to perform qualitative data analysis?

- A. Finding links between data and discover threat-related information
- B. Regression analysis, variance analysis, and so on
- C. Brainstorming, interviewing, SWOT analysis, Delphi technique, and so on
- D. Numerical calculations, statistical modeling, measurement, research, and so on.

Answer: C

Explanation:

For Alice to perform qualitative data analysis, techniques such as brainstorming, interviewing, SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis, and the Delphi technique are suitable. Unlike quantitative analysis, which involves numerical calculations and statistical modeling, qualitative analysis focuses on understanding patterns, themes, and narratives within the data. These techniques enable the analyst to explore the data's deeper meanings and insights, which are essential for strategic decision-making and developing a nuanced understanding of cybersecurity threats and vulnerabilities.References:
* "Qualitative Research Methods in Cybersecurity," SANS Institute Reading Room
* "The Delphi Method for Cybersecurity Risk Assessment," by Cybersecurity and Infrastructure Security Agency (CISA)

NEW QUESTION # 78
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 treat 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 profiling and attribution
- B. Threat determination and identification
- C. Threat ranking
- D. System modeling

Answer: A

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 # 79
What term describes the trust establishment process, wherein the first organization relies on a body of evidence presented to the second organization, and the level of trust is contingent upon the degree and quality of evidence provided by the initiating organization?

- A. Validated trust
- B. Mediated trust
- C. Direct historical trust
- D. Mandated trust

Answer: A

Explanation:
The scenario describes a trust establishment process where one organization bases its trust in another on the degree and quality of evidence that the second organization provides. This concept is known as Validated Trust.
Validated Trust is built through the verification and assessment of presented evidence such as certifications, security audits, compliance documentation, or past performance. The higher the credibility and quality of the evidence, the greater the level of trust established.
This type of trust is evidence-based, meaning it does not rely solely on previous interactions or third-party mediation but on verifiable proof provided directly between the entities involved.
Why the Other Options Are Incorrect:
* A. Mandated Trust:This is imposed by regulation, policy, or authority. It is not based on evidence but on obligation or requirement.
* B. Direct Historical Trust:This trust is formed from prior experiences and a consistent history of interactions between the entities. It does not depend on new evidence or documentation.
* D. Mediated Trust:This form of trust is established through an intermediary (such as a trusted third party or certificate authority) who vouches for the credibility of one organization to another.
Conclusion:

The process where trust is established based on the degree and quality of evidence provided by one party is known as Validated Trust.
Final Answer: C. Validated Trust
Explanation Reference (Based on CTIA Study Concepts):
According to the CTIA study topics under "Information Sharing and Trust Establishment," validated trust is the level of confidence gained through verification of tangible evidence, certifications, or attestations demonstrating security assurance and reliability.

NEW QUESTION # 80
Sean works as a threat intelligence analyst. He is assigned a project for information gathering on a client's network to find a potential threat. He started analysis and was trying to find out the company's internal URLs, looking for any information about the different departments and business units. He was unable to find any information.
What should Sean do to get the information he needs?

- A. Sean should use online services such as netcraft.com to find the company's internal URLs
- B. Sean should use WayBackMachine in Archive.org to find the company's internal URLs
- C. Sean should use e-mail tracking tools such as EmailTrackerPro to find the company's internal URLs
- D. Sean should use website mirroring tools such as HTTrack Web Site Copier to find the company's internal URLs

Answer: A

Explanation:
The goal is to find internal URLs and information about the company's departments and business units.
Since Sean could not find this data directly from public searches, he should turn to online reconnaissance services that provide details about a website's subdomains, internal URLs, hosting structure, and related information.
Netcraft.com is a well-known online reconnaissance and intelligence-gathering service used by security analysts to gather information such as:
* Website structure and internal subdomains
* Server details and operating systems
* Hosting provider and IP ranges
* Technology stack and SSL certificate data
* Historical hosting changes and DNS information
Using Netcraft, Sean can discover internal URLs and subdomains that may reveal internal departments or services linked to the main organization's domain. This type of open-source intelligence (OSINT) is valuable for both threat hunting and vulnerability assessment.
Why the Other Options Are Incorrect:
* A. WayBackMachine (Archive.org):Useful for viewing historical versions of web pages, but it typically shows public pages, not internal or hidden URLs.
* B. Email tracking tools (EmailTrackerPro):These are designed to trace email origins and headers, not to discover website URLs or internal structures.
* C. Website mirroring tools (HTTrack):These tools copy the visible contents of a website but do not reveal hidden internal URLs unless they are publicly linked.
Conclusion:
The correct method for Sean to identify internal URLs and subdomains of the target company is by using online services such as Netcraft.com.
Final Answer: D. Sean should use online services such as netcraft.com to find the company's internal URLs Explanation Reference (Based on CTIA Study Concepts):
According to CTIA study material on Footprinting and Reconnaissance, Netcraft is an effective OSINT- based platform used for discovering detailed website information, including subdomains, server data, and hosting infrastructure.

NEW QUESTION # 81
Sam works as an analyst in an organization named InfoTech Security. He was asked to collect information from various threat intelligence sources. In meeting the deadline, he forgot to verify the threat intelligence sources and used data from an open-source data provider, who offered it at a very low cost. Through it was beneficial at the initial stage but relying on such data providers can produce unreliable data and noise putting the organization network into risk.
What mistake Sam did that led to this situation?

- A. Sam did not use the proper standardization formats for representing threat data.
- B. Sam used data without context.

- C. Sam did not use the proper technology to use or consume the information.
- D. Sam used unreliable intelligence sources.

Answer: D

Explanation:
Sam's mistake was using threat intelligence from sources that he did not verify for reliability. Relying on intelligence from unverified or unreliable sources can lead to the incorporation of inaccurate, outdated, or irrelevant information into the organization's threat intelligence program. This can result in "noise," which refers to irrelevant or false information that can distract from real threats, and potentially put the organization's network at risk. Verifying the credibility and reliability of intelligence sources is crucial to ensure that the data used for making security decisions is accurate and actionable.
References:
"Best Practices for Threat Intelligence Sharing," by FIRST (Forum of Incident Response and Security Teams)
"Evaluating Cyber Threat Intelligence Sources," by Jon DiMaggio, SANS Institute InfoSec Reading Room

NEW QUESTION # 82
.....