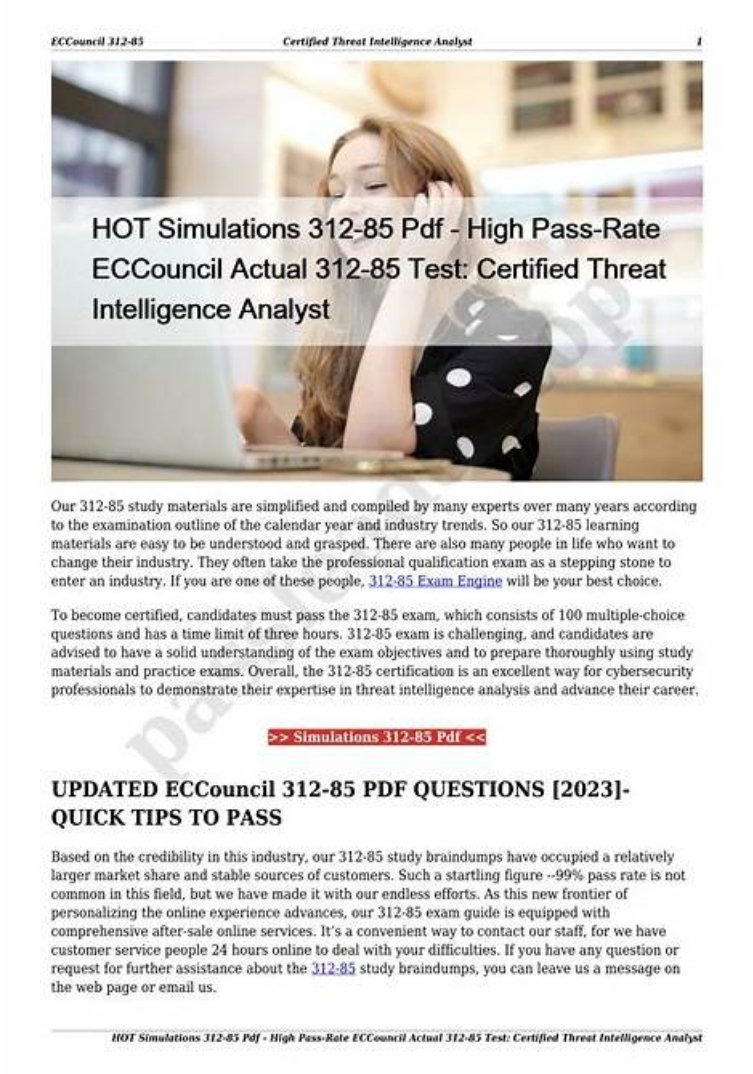
Pdf 312-85 Braindumps, 312-85 New Real Test



BONUS!!! Download part of PDFBraindumps 312-85 dumps for free: https://drive.google.com/open?id=1dId-beYQyKmLuy67XGmJiAMt-MAQq5pI

Do you want to pass 312-85 exam in one time? PDFBraindumps exists for the purpose of fulfilling your will, and it will be your best choice because it can meet your needs. After you buy our 312-85 Dumps, we promise you that we will offer free update service in one year. If you fail the exam, we also promise full refund.

As you see, all of the three versions are helpful for you to get the 312-85 certification: the PDF, Software and APP online. So there is another choice for you to purchase the comprehensive version which contains all the three formats, it is the Value Pack. Besides, the price for the Value Pack is quite favorable. And no matter which format of 312-85 study engine you choose, we will give you 24/7 online service and one year's free updates on the 312-85 practice questions.

>> Pdf 312-85 Braindumps <<

312-85 New Real Test, Valid 312-85 Exam Duration

PDFBraindumps offers verified, authentic ECCouncil 312-85 Real Questions and answers, which are essential for passing the Certified Threat Intelligence Analyst (312-85). These questions and answers have been designed by Sitecore experts and can be easily downloaded on a PC, MacBook, or smartphone for comfortable and convenient learning.

The CTIA certification is ideal for a wide range of professionals, including cybersecurity analysts, threat intelligence analysts, incident

responders, security operations center (SOC) analysts, and security consultants. It is also suitable for professionals working in the government, military, law enforcement, and intelligence agencies. Certified Threat Intelligence Analyst certification is vendor-neutral, meaning that it is not tied to any specific product or technology, making it applicable to a wide range of organizations.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q61-Q66):

NEW QUESTION # 61
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. related: www.infothech.org
- B. cache: www.infothech.org
- C. link: www.infothech.org
- D. info: www.infothech.org

Answer: A

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 # 62
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. System modeling
- B. Threat profiling and attribution
- C. Threat ranking
- D. Threat determination and identification

Answer: B

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 # 63
Kira works as a security analyst in an organization. She was asked to define and set up the requirements before collecting threat

intelligence information. The requirements should focus on what must be collected in order to fulfil production intelligence.
Which of the following categories of threat intelligence requirements should Kira focus on?

- A. Collection requirements
- B. Business requirements
- C. Production requirements
- D. Intelligence requirements

Answer: D

Explanation:
The phase described involves defining and setting up what intelligence needs to be collected before the actual collection process begins. This aligns with the Intelligence Requirements phase of the threat intelligence lifecycle.
Intelligence Requirements define what information is needed and why it is needed to support decision- making or intelligence production. These requirements guide the collection and analysis processes by specifying the goals and priorities of intelligence gathering.
Kira's focus should be on determining the exact intelligence needs that will later drive the production of actionable insights.
Why the Other Options Are Incorrect:
* A. Production requirements: Concerned with how intelligence reports and outputs will be formatted and disseminated after analysis, not what data should be collected.
* C. Business requirements: Focus on organizational goals or project objectives, not specific intelligence needs.
* D. Collection requirements: Define how and from where to gather data, but are based on intelligence requirements, which come first.
Conclusion:
Kira should define Intelligence Requirements, which determine what must be collected to fulfill intelligence production needs.
Final Answer: B. Intelligence requirements
Explanation Reference (Based on CTIA Study Concepts):
In the CTIA threat intelligence lifecycle, defining intelligence requirements is the first stage and establishes the foundation for effective intelligence collection and production.

NEW QUESTION # 64
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. Tactical threat intelligence
- B. Strategic threat intelligence
- C. Operational threat intelligence
- D. Technical threat intelligence

Answer: A

NEW QUESTION # 65
Enrage Tech Company hired Enrique, a security analyst, for performing threat intelligence analysis. While performing data collection process, he used a counterintelligence mechanism where a recursive DNS server is employed to perform interserver DNS communication and when a request is generated from any name server to the recursive DNS server, the recursive DNS servers log the responses that are received. Then it replicates the logged data and stores the data in the central database. Using these logs, he analyzed the malicious attempts that took place over DNS infrastructure.
Which of the following cyber counterintelligence (CCI) gathering technique has Enrique used for data collection?

- A. Data collection through dynamic DNS (DDNS)
- B. Data collection through DNS interrogation
- C. Data collection through DNS zone transfer
- D. Data collection through passive DNS monitoring

Answer: D

Explanation:

Passive DNS monitoring involves collecting data about DNS queries and responses without actively querying DNS servers, thereby not altering or interfering with DNS traffic. This technique allows analysts to track changes in DNS records and observe patterns that may indicate malicious activity. In the scenario described, Enrique is employing passive DNS monitoring by using a recursive DNS server to log the responses received from name servers, storing these logs in a central database for analysis. This approach is effective for identifying malicious domains, mapping malware campaigns, and understanding threat actors' infrastructure without alerting them to the fact that they are being monitored. This method is distinct from active techniques such as DNS interrogation or zone transfers, which involve sending queries to DNS servers, and dynamic DNS, which refers to the automatic updating of DNS records.
References:
SANS Institute InfoSec Reading Room, "Using Passive DNS to Enhance Cyber Threat Intelligence"
"Passive DNS Replication," by Florian Weimer, FIRST Conference Presentation

NEW QUESTION # 66
......