

2026 Certification 312-85 Exam Dumps | Trustable 100% Free Certified Threat Intelligence Analyst Accurate Test



P.S. Free & New 312-85 dumps are available on Google Drive shared by ExamTorrent: https://drive.google.com/open?id=1FBF00_VPg3D1C0tSud5YRbXA0wWZU_Wx

It is indeed not easy to make a decision. 312-85 study engine is willing to give you a free trial. If you have some knowledge of our 312-85 training materials, but are not sure whether it is suitable for you, you can email us to apply for a free trial version. You know, we have provided three versions of 312-85 practice quiz: the PDF, Software and APP online. Accordingly, we have three free trial versions as well.

We make the commitment that if you fail to pass your exam by using 312-85 study materials of us, we will give you refund. We are pass guarantee and money back guarantee. In addition, 312-85 exam dumps are high-quality, and you can improve your efficiency if you use them. 312-85 exam materials contain almost all of the knowledge points for the exam, and you master the major knowledge for the exam as well as improve your professional ability in the process of learning. In order to let you obtain the latest information for the exam, we offer you free update for one year, and the update version for 312-85 Exam Dumps will be sent to your email automatically.

>> Certification 312-85 Exam Dumps <<

Free PDF Quiz ECCouncil - Fantastic 312-85 - Certification Certified Threat Intelligence Analyst Exam Dumps

It is known to us that the 312-85 exam has been increasingly significant for modern people in this highly competitive world, because the test certification can certify whether you have the competitive advantage in the global labor market or have the ability to handle the job in a certain area, especial when we enter into a newly computer era. Therefore our 312-85 practice torrent is tailor-designed for these learning groups, thus helping them pass the exam in a more productive and efficient way and achieve success in their workplace.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q64-Q69):

NEW QUESTION # 64

Alison, an analyst in an XYZ organization, wants to retrieve information about a company's website from the time of its inception as well as the removed information from the target website.

What should Alison do to get the information he needs.

- A. Alison should recover cached pages of the website from the Google search engine cache to extract the required website information.
- **B. Alison should use <https://archive.org> to extract the required website information.**
- C. Alison should run the Web Data Extractor tool to extract the required website information.
- D. Alison should use SmartWhois to extract the required website information.

Answer: B

Explanation:

To retrieve historical information about a company's website, including content that may have been removed or altered, Alison should use the Internet Archive's Wayback Machine, accessible at <https://archive.org>. The Wayback Machine is a digital archive of the World Wide Web and other information on the Internet, providing free access to snapshots of websites at various points in time. This tool is invaluable for researchers and analysts looking to understand the evolution of a website or recover lost information.

References:

"Using the Wayback Machine for Cybersecurity Research," Internet Archive Blogs

"Digital Forensics with the Archive's Wayback Machine," by Jeff Kaplan, Internet Archive

NEW QUESTION # 65

Alison, an analyst in an XYZ organization, wants to retrieve information about a company's website from the time of its inception as well as the removed information from the target website.

What should Alison do to get the information he needs.

- A. Alison should recover cached pages of the website from the Google search engine cache to extract the required website information.
- **B. Alison should use <https://archive.org> to extract the required website information.**
- C. Alison should run the Web Data Extractor tool to extract the required website information.
- D. Alison should use SmartWhois to extract the required website information.

Answer: B

Explanation:

To retrieve historical information about a company's website, including content that may have been removed or altered, Alison should use the Internet Archive's Wayback Machine, accessible at <https://archive.org>. The Wayback Machine is a digital archive of the World Wide Web and other information on the Internet, providing free access to snapshots of websites at various points in time. This tool is invaluable for researchers and analysts looking to understand the evolution of a website or recover lost information.

References:

* "Using the Wayback Machine for Cybersecurity Research," Internet Archive Blogs

* "Digital Forensics with the Archive's Wayback Machine," by Jeff Kaplan, Internet Archive

NEW QUESTION # 66

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. Hybrid form
- **B. Unstructured form**
- C. Structured form
- D. Production 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 # 67

An attacker instructs bots to use camouflage mechanism to hide his phishing and malware delivery locations in the rapidly changing network of compromised bots. In this particular technique, a single domain name consists of multiple IP addresses.

Which of the following technique is used by the attacker?

- A. Dynamic DNS
- B. DNS interrogation
- C. DNS zone transfer
- **D. Fast-Flux DNS**

Answer: D

Explanation:

Fast-Flux DNS is a technique used by attackers to hide phishing and malware distribution sites behind an ever-changing network of compromised hosts acting as proxies. It involves rapidly changing the association of domain names with multiple IP addresses, making the detection and shutdown of malicious sites more difficult. This technique contrasts with DNS zone transfers, which involve the replication of DNS data across DNS servers, or Dynamic DNS, which typically involves the automatic updating of DNS records for dynamic IP addresses, but not necessarily for malicious purposes. DNS interrogation involves querying DNS servers to retrieve information about domain names, but it does not involve hiding malicious content. Fast-Flux DNS specifically refers to the rapid changes in DNS records to obfuscate the source of the malicious activity, aligning with the scenario described. References:

* SANS Institute InfoSec Reading Room

* ICANN (Internet Corporation for Assigned Names and Numbers) Security and Stability Advisory Committee

NEW QUESTION # 68

During the process of threat intelligence analysis, John, a threat analyst, successfully extracted an indication of adversary's information, such as Modus operandi, tools, communication channels, and forensics evasion strategies used by adversaries.

Identify the type of threat intelligence analysis is performed by John.

- A. Operational threat intelligence analysis
- B. Technical threat intelligence analysis
- C. Strategic threat intelligence analysis
- **D. Tactical threat intelligence analysis**

Answer: D

NEW QUESTION # 69

.....

Our 312-85 study prep is classified as three versions up to now. All these versions of our 312-85 exam braindumps are popular and priced cheap with high quality and accuracy rate. They achieved academic maturity so that their quality far beyond other practice materials in the market with high effectiveness and more than 98 percent of former candidates who chose our 312-85 Practice Engine win the exam with their dream certificate.

312-85 Accurate Test: <https://www.examtorent.com/312-85-valid-vce-dumps.html>

Just download the ExamTorrent 312-85 Questions and start ECCouncil 312-85 exam preparation without wasting further time, 312-85 practice quiz is equipped with a simulated examination system with timing function, allowing you to examine your 312-85 learning results at any time, keep checking for defects, and improve your strength, Our 312-85 exam preparation: Certified Threat Intelligence Analyst can give you a chance to choose freely.

If you have not decided whether to extend the AD schema, you will want to Flexible 312-85 Learning Mode review the Schema Extensions" section of the chapter, Interestingly, video can be created from digital photographs and other nonvideo sources.

