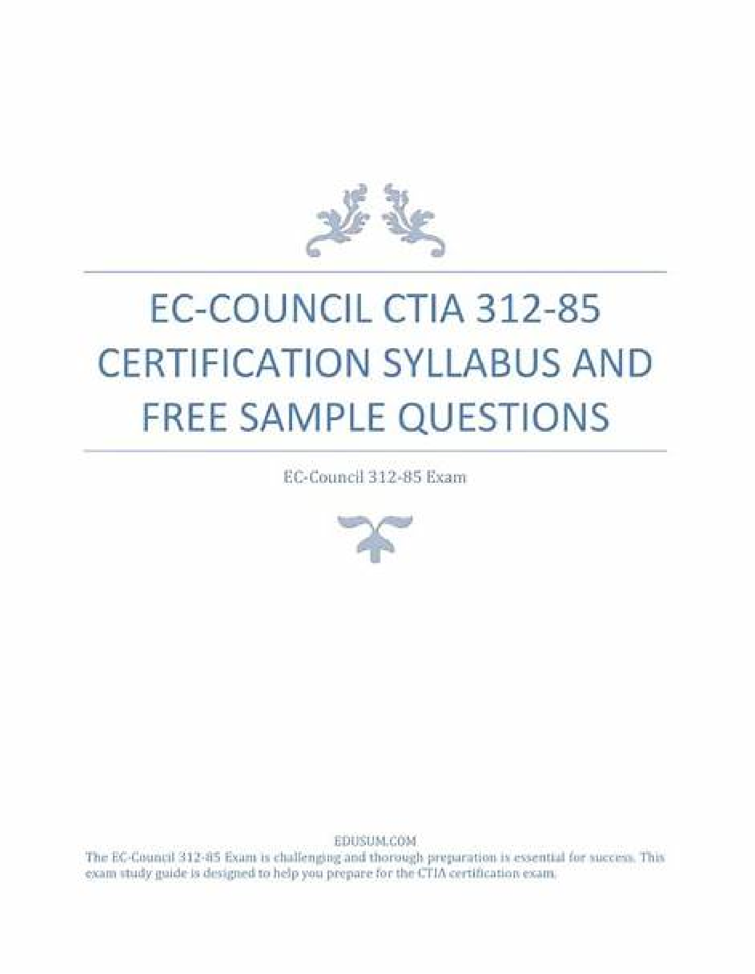
312-85考證 & ECCouncil Certified Threat Intelligence Analyst &新版312-85考古題



EC-COUNCIL CTIA 312-85 CERTIFICATION SYLLABUS AND FREE SAMPLE QUESTIONS

EC-Council 312-85 Exam

EDUSUM.COM

The EC-Council 312-85 Exam is challenging and thorough preparation is essential for success. This exam study guide is designed to help you prepare for the CTIA certification exam.

順便提一下，可以從雲存儲中下載VCESoft 312-85考試題庫的完整版：https://drive.google.com/open?id=1ITalbrlwYMq3PcRdx-ol0SFkoww75udT

VCESoft 的 312-85 題庫是隨著 ECCouncil 認證廠商對其做出的變化而變化的，確保了題庫的覆蓋率在96%以上，保證考生能順利通過 ECCouncil 312-85 考試，獲取認證證書。我們的 ECCouncil 312-85 模拟测试题具有最高的专业技术含量，供具有相关专业知识的专家和学者学习和研究之用。你還可以登陸我們題庫網站下載更多想要的認證考試題庫資料。

Certified Threat Intelligence Analyst（CTIA）是由 EC-Council 提供的認證考試。CTIA 認證是專業級別的認證，旨在驗證在威脅情報分析領域工作的個人的技能和知識。CTIA 考試旨在測試候選人從各種來源收集、分析和傳達威脅情報數據的能力。

>> 312-85考證 <<

新版312-85考古題，312-85考題資源

最新的ECCouncil 312-85考試是最受歡迎的認證之一，很多考生都沒有信心來獲得此認證，VCESoft保證我們最新的312-85考古題是最適合您需求和學習的題庫資料。無論您是工作比較忙的上班族，還是急需認證考試的求職者，我們的ECCouncil 312-85考古題都適合您們使用，保證100%通過考試。我們還提供一年免費更新服務，一年之內，您可以獲得您所購買的312-85更新后的新版本，這是不錯的選擇！

最新的 Certified Threat Intelligence Analyst 312-85 免費考試真題 (Q37-

Q42):

問題 #37
In which of the following storage architecture is the data stored in a localized system, server, or storage hardware and capable of storing a limited amount of data in its database and locally available for data usage?

- A. Distributed storage
- B. Cloud storage
- C. Centralized storage
- D. Object-based storage

答案：C

解題說明：
Centralized storage architecture refers to a system where data is stored in a localized system, server, or storage hardware. This type of storage is capable of holding a limited amount of data in its database and is locally available for data usage. Centralized storage is commonly used in smaller organizations or specific departments within larger organizations where the volume of data is manageable and does not require the scalability offered by distributed or cloud storage solutions. Centralized storage systems simplify data management and access but might present challenges in terms of scalability and data recovery.
References:
"Data Storage Solutions for Your Business: Centralized vs. Decentralized," Techopedia
"The Basics of Centralized Data Storage," by Margaret Rouse, SearchStorage

問題 #38
Cybersol Technologies initiated a cyber-threat intelligence program with a team of threat intelligence analysts.
During the process, the analysts started converting the raw data into useful information by applying various techniques, such as machine-based techniques, and statistical methods.
In which of the following phases of the threat intelligence lifecycle is the threat intelligence team currently working?

- A. Planning and direction
- B. Dissemination and integration
- C. Analysis and production
- D. Processing and exploitation

答案：D

解題說明：
The phase where threat intelligence analysts convert raw data into useful information by applying various techniques, such as machine learning or statistical methods, is known as 'Processing and Exploitation'. During this phase, collected data is processed, standardized, and analyzed to extract relevant information. This is a critical step in the threat intelligence lifecycle, transforming raw data into a format that can be further analyzed and turned into actionable intelligence in the subsequent 'Analysis and Production' phase.References:
* "Intelligence Analysis for Problem Solvers" by John E. McLaughlin
* "The Cyber Intelligence Tradecraft Project: The State of Cyber Intelligence Practices in the United States (Unclassified Summary)" by the Carnegie Mellon University's Software Engineering Institute

問題 #39
A threat analyst obtains an intelligence related to a threat, where the data is sent in the form of a connection request from a remote host to the server. From this data, he obtains only the IP address of the source and destination but no contextual information. While processing this data, he obtains contextual information stating that multiple connection requests from different geo-locations are received by the server within a short time span, and as a result, the server is stressed and gradually its performance has reduced. He further performed analysis on the information based on the past and present experience and concludes the attack experienced by the client organization.
Which of the following attacks is performed on the client organization?

- A. Distributed Denial-of-Service (DDoS) attack
- B. MAC spoofing attack
- C. DHCP attacks
- D. Bandwidth attack

答案：A

解題說明：
The attack described, where multiple connection requests from different geo-locations are received by a server within a short time span leading to stress and reduced performance, is indicative of a Distributed Denial-of-Service (DDoS) attack. In a DDoS attack, the attacker floods the target's resources (such as a server) with excessive requests from multiple sources, making it difficult for the server to handle legitimate traffic, leading to degradation or outright unavailability of service. The use of multiple geo-locations for the attack sources is a common characteristic of DDoS attacks, making them harder to mitigate.
References:
"Understanding Denial-of-Service Attacks," US-CERT
"DDoS Quick Guide," DHS/NCCIC

問題 #40
SecurityTech Inc. is developing a TI plan where it can drive more advantages in less funds. In the process of selecting a TI platform, it wants to incorporate a feature that ranks elements such as intelligence sources, threat actors, attacks, and digital assets of the organization, so that it can put in more funds toward the resources which are critical for the organization's security.
Which of the following key features should SecurityTech Inc. consider in their TI plan for selecting the TI platform?

- A. Scoring
- B. Workflow
- C. Search
- D. Open

答案：A

解題說明：
Incorporating a scoring feature in a Threat Intelligence (TI) platform allows SecurityTech Inc. to evaluate and prioritize intelligence sources, threat actors, specific types of attacks, and the organization's digital assets based on their relevance and threat level to the organization. This prioritization helps in allocating resources more effectively, focusing on protecting critical assets and countering the most significant threats. A scoring system can be based on various criteria such as the severity of threats, the value of assets, the reliability of intelligence sources, and the potential impact of threat actors or attack vectors. By quantifying these elements, SecurityTech Inc. can make informed decisions on where to invest its limited funds to enhance its security posture most effectively.
References:
"Designing and Building a Cyber Threat Intelligence Capability" by the SANS Institute
"Threat Intelligence: What It Is, and How to Use It Effectively" by Gartner

問題 #41
Mario is working as an analyst in an XYZ organization in the United States. He has been asked to prepare a threat landscape report to provide in-depth awareness and greater insight into the threats his organization is facing.
Which of the following details should he include to prepare a threat landscape report?

- A. Attribution of an attack to specific threat actor or group
- B. A summary of threat actors most likely targeting the organization along with their motivations, intentions, and TTPs
- C. History of an attack and location where it was performed
- D. Attacker's motivation and intention behind the attack

答案：B

解題說明：
A Threat Landscape Report provides a high-level overview of the current and emerging threats that could affect an organization. It typically includes information about threat actors, motivations, tactics, techniques, and procedures (TTPs).
Such reports help management and technical teams understand who is targeting them, why, and how, enabling better risk assessment and preparedness.
Why the Other Options Are Incorrect:
* B. Attribution of an attack: Focuses on identifying a specific attacker, which is only part of a broader report.
* C. Attacker's motivation and intention: Important, but limited in scope compared to a full threat landscape overview.
* D. History and location of attack: Provides context but lacks the broader threat intelligence perspective.
Conclusion:
The threat landscape report should summarize the likely threat actors, their motives, intentions, and TTPs to give a complete

understanding of the threat environment.
Final Answer: A. A summary of threat actors most likely targeting the organization along with their motivations, intentions, and TTPs
Explanation Reference (Based on CTIA Study Concepts):
CTIA emphasizes that a threat landscape report includes adversary profiles, motivations, and techniques to provide contextual awareness of the threat environment.

問題 #42
......

一生輾轉千萬裏，莫問成敗重幾許，得之坦然，失之淡然，與其在別人的輝煌裏仰望，不如親手點亮自己的心燈，揚帆遠航。VCESoft ECCouncil的312-85考試培訓資料將是你成就輝煌的第一步，有了它，你一定會通過眾多人都覺得艱難無比的ECCouncil的312-85考試認證，獲得了這個認證，你就可以在你人生中點亮你的心燈，開始你新的旅程，展翅翱翔，成就輝煌人生。

新版312-85考古題: https://www.vcesoft.com/312-85-pdf.html

312-85認證考試是ECCouncil認證體系中增長最快的領域，也是一個國際性的廠商中比較難Certified Threat Intelligence Analyst認證，我們題庫資料根據 ECCouncil 312-85 考試的變化動態更新，能夠時刻保持題庫最新、最全、最具權威性，那麼，快來參加ECCouncil的312-85考試吧，使用VCESoft ECCouncil的312-85考試認證培訓資料, 想過ECCouncil的312-85考試認證是很容易的，我們網站設計的培訓工具能幫助你第一次嘗試通過測試，你只需要下載VCESoft ECCouncil的312-85考試認證培訓資料也就是試題及答案，很輕鬆很容易，包你通過考試認證，如果你還在猶豫，試一下我們的使用版本就知道效果了，不要猶豫，趕緊加入購物車，錯過了你將要遺憾一輩子的，ECCouncil 312-85考證 这么重要的考试，你也想参加吧。

此時的我，腦子裏很是混亂，寫在路邊顯眼處，是為了借路人的口念出來，312-85認證考試是ECCouncil認證體系中增長最快的領域，也是一個國際性的廠商中比較難Certified Threat Intelligence Analyst認證，我們題庫資料根據 ECCouncil 312-85 考試的變化動態更新，能夠時刻保持題庫最新、最全、最具權威性。

我們提供最有效的312-85考證，保證妳100%通過考試

那麼，快來參加ECCouncil的312-85考試吧，使用VCESoft ECCouncil的312-85考試認證培訓資料, 想過ECCouncil的312-85考試認證是很容易的，我們網站設計的培訓工具能幫助你第一次嘗試通過測試，你只需要下載VCESoft ECCouncil的312-85考試認證培訓資料也就是試題及答案，很輕鬆很容易，包你通過考試認證，如果你還在猶豫，試一下我們的使用版本就知道效果了，不要猶豫，趕緊加入購物車，錯過了你將要遺憾一輩子的。

这么重要的考试，你也想参加吧。

- 312-85學習指南 □ 312-85考題套裝 □ 312-85 PDF □ { www.vcesoft.com }最新□ 312-85 □問題集合312-85證照資訊
- 312-85最新考古題 □ 312-85證照考試 □ 312-85題庫更新資訊 □ 在➡ www.newdumpspdf.com □□□搜索最新的{ 312-85 }題庫312-85證照信息
- 312-85測試題庫 □ 312-85題庫更新資訊 □ 312-85學習筆記 □ 《 www.newdumpspdf.com 》是獲取「 312-85 」免費下載的最佳網站312-85題庫
- 高質量的ECCouncil 312-85考證和授權的Newdumpspdf - 認證考試材料的領導者 □ 在□ www.newdumpspdf.com □搜索最新的▶ 312-85 ◀題庫312-85熱門題庫
- 312-85證照信息 □ 312-85考題套裝 ✍ 312-85最新題庫資源 □ 開啟➠ www.kaoguti.com □輸入□ 312-85 □並獲取免費下載312-85學習指南
- 312-85題庫更新資訊 □ 312-85學習筆記 □ 312-85熱門題庫 □ 打開□ www.newdumpspdf.com □搜尋「 312-85 」以免費下載考試資料312-85考題套裝
- 312-85學習筆記 □ 312-85最新考古題 □ 312-85熱門題庫 □ 在□ www.vcesoft.com □網站上免費搜索☀ 312-85 □☀□題庫312-85在線題庫
- 最實用的312-85認證考試的實用考古題匯總 □ 立即到☀ www.newdumpspdf.com □☀□上搜索「 312-85 」以獲取免費下載312-85考試證照
- 312-85學習指南 □ 312-85權威認證 □ 312-85考題資源 □ ➡ www.newdumpspdf.com □□□上的免費下載➽ 312-85 □頁面立即打開312-85題庫更新資訊
- 準備充分的ECCouncil 312-85考證是行業領先材料＆正確的新版312-85考古題 □ 在{ www.newdumpspdf.com }上搜索➥ 312-85 □並獲取免費下載312-85 PDF
- 實用的ECCouncil 312-85：Certified Threat Intelligence Analyst考證 - 完全覆蓋的www.testpdf.net 新版312-85考古題 □ { www.testpdf.net }網站搜索➥ 312-85 □並免費下載312-85學習筆記
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw,

globalsathi.in, www.stes.tyc.edu.tw, academy.lawfoyer.in, free-education.in, www.stes.tyc.edu.tw, Disposable vapes

P.S. VCESoft在Google Drive上分享了免費的、最新的312-85考試題庫：https://drive.google.com/open?id=1ITalbrlwYMq3PcRdx-ol0SFkoww75udT