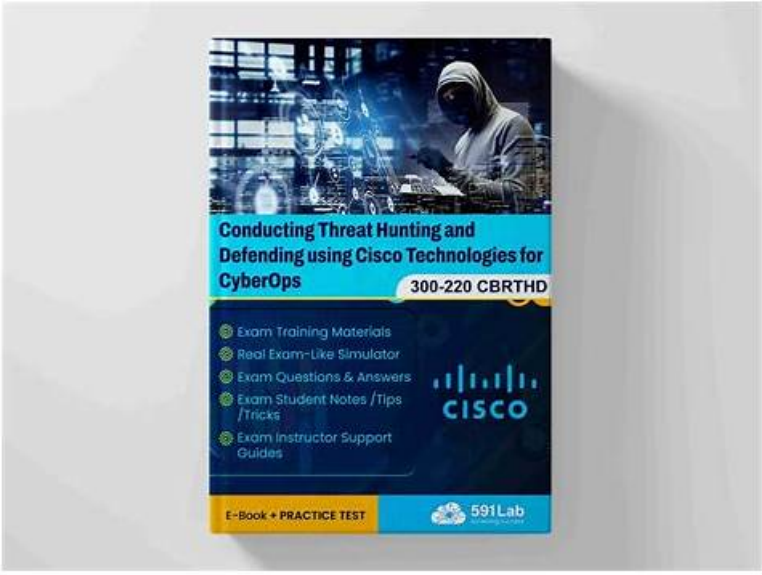
保證通過的Cisco 300-220題庫最新資訊是行業領先材料＆100％合格率的300-220：Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps



2026 NewDumps最新的300-220 PDF版考試題庫和300-220考試問題和答案免費分享：https://drive.google.com/open?id=1py3_zo2sr5oAls3HLfylLO2ZfYHcrxlD

NewDumps不僅能為那你節約寶貴的時間，還可以讓你安心地參加考試以及順利的通過。NewDumps具有很好的可靠性，在專業IT行業人士中有很高的聲譽。你可以通過免費下載我們的NewDumps提供的部分關於Cisco 300-220考題及答案作為嘗試來確定我們的可靠性，相信你會很滿意的。我對我們NewDumps的產品有信心，相信很快NewDumps的關於Cisco 300-220考題及答案就會成為你的不二之選。你也會很快很順利的通過Cisco 300-220的認證考試。選擇我們NewDumps是明智的，NewDumps會是你想要的滿意的產品。

Cisco 300-220 認證考試旨在測試候選人在使用 Cisco 技術進行威脅狩獵和防禦方面的知識和技能。這個認證適用於 CyberOps 專業人員，他們希望提高在識別和緩解網絡安全威脅方面的專業知識。考試涵蓋一系列主題，包括威脅情報概念、安全操作基礎知識、網絡基礎架構安全、端點保護和事件響應。

>> 300-220題庫最新資訊 <<

300-220考題免費下載 - 300-220認證資料

NewDumps 的 300-220 考題和答案是最新的，由最新的考試指南編訂，增加了考生通過考試的概率。是最好的自學教材和習題集，幫助你快速通過 300-220 考試，實現順速獲取證書的最佳捷徑。如果300-220 題庫有變化我們可以第一時間得知，并迅速更新 Cisco 300-220 題庫。如果在考試過程中變題了，考生可以享受免費更新的服務。免費更新一年的 300-220 考題服務。

思科300-220考試適用於從事網路安全運營角色，例如安全分析師、威脅獵人、網路安全工程師和事件應對人員等人士。該考試驗證候選人使用思科技術識別安全威脅、調查安全事件以及抵禦網路攻擊的能力。它也測試候選人對業界標準安全實踐的理解以及他們在實際情況下應用它們的能力。

為了準備 Cisco 300-220 考試，考生應該擁有扎實的網絡安全背景，包括安全原理、協議和技術的知識。他們還應該有使用 Cisco 技術（包括防火牆、入侵防止系統和其他安全工具）的經驗。此外，考生應該有進行威脅獵捕和事件響應活動的經驗，以及分析安全事件和識別潛在威脅的能力。

最新的 CyberOps Associate 300-220 免費考試真題 (Q120-Q125):

問題 #120
Which threat modeling standard encompasses various phases of the attack lifecycle, from planning to execution?

- A. TaHiTI
- B. MITRE CAPEC
- C. All of the above
- D. PASTA

答案：B

問題 #121
Refer to the exhibit.
A forensic team must investigate how the company website was defaced. The team isolates the web server, clones the disk, and analyzes the logs. Which technique was used by the attacker initially to access the website?

- A. exploit public-facing application
- B. drive-by compromise
- C. external remote services
- D. command and scripting interpreter

答案：A

解題說明：
The correct answer isExploit public-facing application. The log excerpt in the exhibit clearly shows a malicious HTTP GET requesttargeting aWordPress plugin PHP filewith a craftedSQL injection payload:
UNION ALL SELECT CONCAT(...)
This syntax is a classic indicator ofSQL injection, a well-documented attack technique used to exploit insufficient input validation in web applications. According to the MITRE ATT&CK framework, this behavior maps to theInitial Access tactic (TA0001)and the techniqueExploit Public-Facing Application (T1190). The attacker is directly interacting with a publicly accessible web service and abusing a vulnerability in the application code to gain unauthorized access.
From a threat hunting and forensic standpoint, this is a textbook example of how attackers commonly achieve initial access to web servers. The attacker did not authenticate via remote services (such as SSH or RDP), nor did they rely on user interaction (as in a drive-by compromise). Instead, they sent a specially crafted request to a vulnerable endpoint exposed to the internet. This makes option B incorrect becauseExternal Remote Servicesrequires legitimate service access mechanisms. Option C is also incorrect becauseCommand and Scripting Interpreteris typically usedafterinitial access, once code execution is already achieved. Option D does not apply because there is no evidence of malicious content being delivered to end users.
The forensic team's actions-isolating the server, cloning the disk, and analyzing logs-are standard post- incident procedures to reconstruct the attack chain. Web server access logs are especially valuable in these cases, as they often reveal malicious payloads, attacker IP addresses, targeted endpoints, and timestamps.
For defenders and threat hunters, this scenario reinforces the importance of monitoring web logs for anomalous query strings, enforcing secure coding practices, conducting regular vulnerability scans, and promptly patching third-party plugins. Public-facing applications remain one of themost exploited initial access vectors, making this technique a critical focus area in modern threat hunting programs.

問題 #122
What is the key difference between threat hunting and traditional cybersecurity measures?

- A. Threat hunting involves actively searching for threats
- B. Threat hunting is reactive
- C. Traditional cybersecurity measures are proactive
- D. Threat hunting only focuses on known threats

答案：A

問題 #123
What disadvantage does automation in security operations face?

- A. It reduces the need for cybersecurity policies
- B. It may struggle with new and unknown threats
- C. It can replace human intuition and decision-making

- D. It can identify all types of malware without updates

答案：B

問題 #124
Which of the following is NOT a typical outcome of successful threat hunting?

- A. Guaranteed prevention of all cyber threats
- B. Identification of new threat indicators
- C. Increased visibility into the security landscape
- D. Improved incident response capabilities

答案：A

問題 #125
......