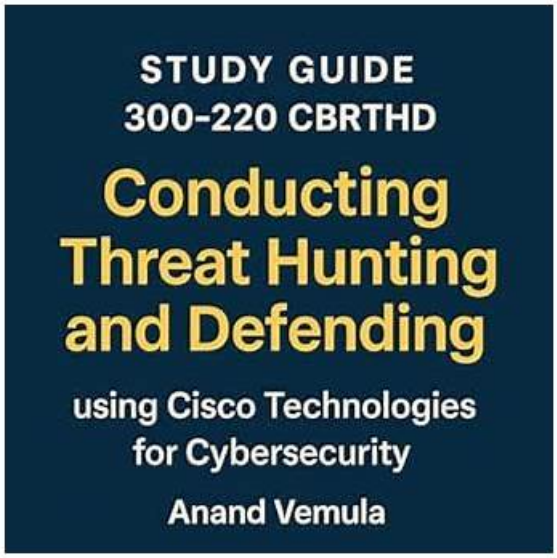
Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps Valid Torrent - 300-220 Training Vce & Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps Latest Pdf



BTW, DOWNLOAD part of ITExamDownload 300-220 dumps from Cloud Storage: https://drive.google.com/open?id=18RB1edw3Vg8laxOxTuBQfNVR816iKDLA

Once you learn all 300-220 questions and answers in the study guide, try ITExamDownload's innovative testing engine for exam like 300-220 practice tests. These tests are made on the pattern of the 300-220 real exam and thus remain helpful not only for the purpose of revision but also to know the real exam scenario. To ensure excellent score in the exam, 300-220 Braindumps are the real feast for all exam candidates. They contain questions and answers on all the core points of your exam syllabus. Most of these questions are likely to appear in the 300-220 real exam.

Cisco 300-220 exam covers a wide range of topics related to cybersecurity and threat hunting. These topics include the detection and analysis of malware, network security, endpoint protection, incident response, and threat intelligence. 300-220 Exam also covers the use of Cisco security technologies such as Firepower, ISE, and Stealthwatch.

>> 300-220 Exam Overviews <<

Test 300-220 Dump - 300-220 Exam Material

In this cut-throat competitive world of ITExamDownload, the Cisco 300-220 certification is the most desired one. But what creates an obstacle in the way of the aspirants of the Cisco 300-220 certificate is their failure to find up-to-date, unique, and reliable 300-220 practice material to succeed in passing the Cisco 300-220 certification exam. If you are one of such frustrated candidates, don't get panic. ITExamDownload declares its services in providing the real 300-220 PDF Questions.

Cisco 300-220 Exam is an essential certification for anyone pursuing a career in cybersecurity. 300-220 exam validates the skills and knowledge required to perform entry-level cybersecurity tasks and is recognized globally as a respected certification. As cyber

attacks become more prevalent and sophisticated, the demand for qualified cybersecurity professionals continues to rise. Obtaining this certification will open up new employment opportunities and demonstrate to employers your dedication to the field of cybersecurity.

Cisco Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps Sample Questions (Q60-Q65):

NEW QUESTION # 60
A threat hunter is usingCisco Secure Network Analytics (Stealthwatch)to investigate possible lateral movement inside the network. Which behavior would MOST strongly indicate lateral movement using valid credentials?

- A. DNS queries to newly registered domains
- B. Repeated HTTP requests to the same external IP address
- C. Internal systems authenticating to multiple hosts using SMB in a short time
- D. High volume of inbound internet traffic to a web server

Answer: C

Explanation:
The correct answer isinternal systems authenticating to multiple hosts using SMB in a short time. This behavior is a classic indicator ofcredential-based lateral movement.
When attackers obtain valid credentials, they often move laterally by:
* Accessing administrative shares (e.g., C$, ADMIN$)
* Using SMB, WMI, WinRM, or RDP
* Authenticating to multiple systems rapidly
Cisco Secure Network Analytics excels at identifyingeast-west traffic anomalies, which are central to lateral movement detection. A single host authenticating to many internal systems over SMB in a short time deviates strongly from normal user behavior.
Option A relates to external traffic, not lateral movement. Option C may indicate command-and-control or staging but not lateral movement. Option D aligns more with beaconing behavior.
This technique aligns withMITRE ATT&CK - Lateral Movementand is explicitly covered in theCBRTHD blueprintunder network-based threat hunting.
Thus,Option Bis the correct answer.

NEW QUESTION # 61
What is the first step in the threat hunting process?

- A. Understanding the organization's environment and assets
- B. Defending against known attacks
- C. Identifying potential threat indicators
- D. Analyzing network traffic

Answer: A

NEW QUESTION # 62
What is the primary goal of threat hunting techniques?

- A. To respond to threats after they have already occurred
- B. To ignore potential threats and focus on other security measures
- C. To rely solely on automated tools for threat detection
- D. To proactively search for potential threats within an organization

Answer: D

NEW QUESTION # 63
What is the purpose of using sandboxing as a threat hunting technique?

- A. To monitor network traffic

- B. To analyze log files
- C. To conduct penetration testing
- D. To analyze malware behavior in a controlled environment

Answer: D

NEW QUESTION # 64
What is an advantage of using behavioral analysis for threat actor attribution?

- A. Allows for tracking of threat actors across different platforms
- B. Offers insights into the motives and strategies of threat actors
- C. Provides real-time identification of threat actors
- D. Can be easily manipulated by threat actors

Answer: B

NEW QUESTION # 65
.....