Quiz 2026 Pass-Sure Cisco 300-220: Pdf Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps Dumps

BONUS!!! Download part of Itcertking 300-220 dumps for free: https://drive.google.com/open?id=1U3siPN6JFwfKUQBSMswuaI-CauE38l8w

In this fast-changing world, the requirements for jobs and talents are higher, and if people want to find a job with high salary they must boost varied skills which not only include the good health but also the working abilities. But if you get the 300-220 certification, your working abilities will be proved and you will find an ideal job. We provide you with 300-220 Exam Materials of high quality which can help you pass the 300-220 exam easily. It also saves your much time and energy that you only need little time to learn and prepare for 300-220 exam.

Cisco 300-220 certification is valuable for individuals who are looking to advance their careers in the cybersecurity industry. It is also a valuable asset for organizations that want to hire cybersecurity professionals with the necessary skills and knowledge to defend against cyber threats. By earning this certification, professionals can demonstrate their commitment to staying up-to-date with the latest cybersecurity technologies and best practices.

Cisco 300-220 exam, also known as Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps, is designed for IT professionals who want to validate their knowledge and skills in threat hunting and defense using Cisco technologies. 300-220 Exam is part of the Cisco CyberOps Associate certification, which aims to develop foundational skills needed for a career in cybersecurity operations.

Earning the Cisco Certified CyberOps Professional certification can help IT professionals advance their careers and demonstrate their expertise in cybersecurity operations. The Cisco 300-220 exam is an essential step towards achieving this certification and is a valuable asset for any cybersecurity professional looking to enhance their skills and knowledge.

>> Pdf 300-220 Dumps <<

Exam 300-220 Torrent | 300-220 Valid Exam Cram

The Cisco 300-220 Dumps PDF File material is printable, enabling your off-screen study. This format is portable and easily usable on smart devices including laptops, tablets, and smartphones. Cisco 300-220 dumps team of professionals keeps an eye on content of the Cisco 300-220 Exam and updates its product accordingly. Our pdf is a very handy format for casual and quick preparation of the Cisco certification exam.

Cisco Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps Sample Questions (Q39-Q44):

NEW QUESTION # 39
To identify unknown gaps in detection, one should:

- A. Rely solely on automated alerts
- B. Conduct regular security assessments
- C. Assume all configurations are secure
- D. Only trust verified threats

Answer: B

NEW QUESTION # 40
In the context of threat hunting, what is the purpose of conducting "incubation"?

- A. To deploy additional security controls
- B. To observe the evolution of attack tactics
- C. To slow down the attack process
- D. To directly confront threat actors

Answer: B

NEW QUESTION # 41
What is the role of hypothesis-driven hunting in threat hunting?

- A. It relies solely on automated tools for threat detection.
- B. It involves randomly searching for threats without any specific goal.
- C. It focuses on forming educated guesses about potential threats and testing them through investigation.
- D. It is not a common practice in threat hunting.

Answer: C

NEW QUESTION # 42
A security team wants to create a plan to protect companies from lateral movement attacks. The team already implemented detection alerts for pass-the-hash and pass-the-ticket techniques. Which two components must be monitored to hunt for lateral movement attacks on endpoints? (Choose two.)

- A. Use of tools and commands to connect to remote shares
- B. Linux file systems for files that have the setuid/setgid bit set
- C. Use of Windows Remote Management
- D. Creation of scheduled task events
- E. Use of the runas command

Answer: A,C

Explanation:
The correct answers areUse of Windows Remote Management (C)andUse of tools and commands to connect to remote shares (E). Both are core mechanisms attackers leverage forlateral movementafter gaining valid credentials through techniques such as pass-the-hash or pass-the-ticket.
Windows Remote Management (WinRM) is a legitimate administrative service used for remote command execution and system management. However, attackers frequently abuse WinRM to move laterally by executing commands on remote endpoints using stolen credentials. From a threat hunting perspective, abnormal WinRM usage-such as execution outside normal administrative hours, from unusual source hosts, or by non-administrative user accounts-is a strong indicator of lateral movement activity.
Similarly, the use of tools and commands to connect to remote shares (such as net use, wmic, SMB-based access, or mounting administrative shares like C$) is a classic lateral movement technique. Attackers use remote shares to transfer tools, stage payloads, and execute malware across systems. Monitoring these activities at the endpoint level helps identify suspicious authentication attempts, unexpected share access, and abnormal file transfers.
Option A (runas) relates more to privilege escalation than lateral movement. Option B is specific to Linux privilege persistence and is not relevant to endpoint lateral movement hunting in this context. Option D (scheduled task creation) is primarily associated with persistence rather than movement between systems.
By monitoring WinRM activity and remote share usage, security teams gain visibility intocredential-based movement, which remains one of the most common and dangerous attacker behaviors in enterprise environments. Effective lateral movement hunting focuses onhow credentials are used, not just how they are stolen.

NEW QUESTION # 43
Which of the following is a key benefit of incorporating threat hunting into a cybersecurity strategy?

- A. Enhanced threat intelligence and visibility
- B. Improved network speed and performance
- C. Reduced need for security training
- D. Increased vulnerability to cyber attacks

Answer: A

NEW QUESTION # 44
.....

Using a smartphone, you may go through the Cisco 300-220 dumps questions whenever and wherever you desire. The 300-220 PDF dumps file is also printable for making handy notes. Itcertking has developed the online Cisco 300-220 practice test to help the candidates get exposure to the actual exam environment. By practicing with web-based Cisco 300-220 Practice Test questions you can get rid of exam nervousness. You can easily track your performance while preparing for the Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps exam with the help of a self-assessment report shown at the end of Cisco 300-220 practice test.

P.S. Free 2026 Cisco 300-220 dumps are available on Google Drive shared by Itcertking: https://drive.google.com/open?id=1U3siPN6JFwfKUQBSMswuaI-CauE38l8w