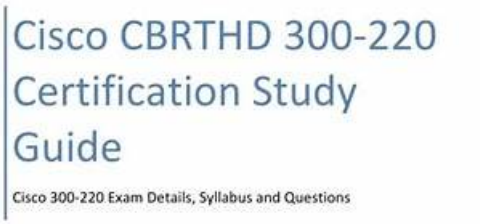
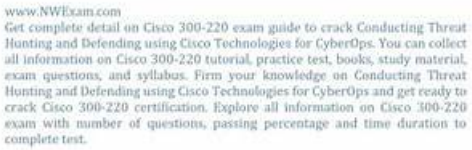
Cisco 300-220 Latest Practice Materials, High 300-220 Quality





P.S. Free & New 300-220 dumps are available on Google Drive shared by It-Tests: https://drive.google.com/open?id=1eriICE1gL6nBDSjtRSAxW6FwuhPrJ8xY

I know you must want to get a higher salary, but your strength must match your ambition! The opportunity is for those who are prepared! 300-220 exam questions can help you improve your strength! You will master the most practical knowledge in the shortest possible time. It is also very easy if you want to get the 300-220 certificate. As long as you buy our 300-220 study braindumps and practice step by step, you are bound to pass the exam.

Cisco 300-220 Exam covers a wide range of topics, including network security, endpoint security, threat intelligence, incident response, and more. Candidates are expected to have a strong understanding of the latest cybersecurity threats and techniques, as well as the ability to use Cisco technologies to secure networks and systems. They must also be able to analyze security events and identify potential threats, and respond to these threats in a timely and effective manner.

>> Cisco 300-220 Latest Practice Materials <<

High Cisco 300-220 Quality, 300-220 Valid Test Book

If you purchase Cisco 300-220 exam questions and review it as required, you will be bound to successfully pass the exam. And if you still don't believe what we are saying, you can log on our platform right now and get a trial version of Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps 300-220 study engine for free to experience the magic of it.

Cisco Conducting Threat Hunting and Defending using Cisco Technologies

for CyberOps Sample Questions (Q130-Q135):

NEW QUESTION # 130
What is the purpose of hypothesis generation in the threat hunting process?

- A. To identify potential threats
- B. To validate known threats
- C. To rule out false positives
- D. To classify threat actors

Answer: A

NEW QUESTION # 131
Selecting deception techniques for a scenario involves:

- A. Sending false positive alerts to attackers
- B. Using misleading comments in the code
- C. Creating fake social media accounts for the IT staff
- D. Placing honeypots within the network

Answer: D

NEW QUESTION # 132
Refer to the exhibit.
A security team detects a spike in traffic from the company web server. After further investigation, the team discovered that multiple connections have been established from the server to different IP addresses, but the web server logs contain both expected traffic and DDoS traffic. Which attribute must the team use to further filter the logs?

- A. protocol
- B. connection status
- C. IP address of the web server
- D. destination port

Answer: B

Explanation:
The correct answer isConnection status. In this scenario, the key challenge for the security team is differentiatinglegitimate outbound trafficfrommalicious or DDoS-related trafficoriginating from the same web server. Since both types of traffic coexist in the logs, analysts must rely on an attribute that meaningfully distinguishes normal behavior from abnormal patterns.
The exhibit shows numerous TCP connections from the web server to many different external IP addresses, with varyingTCP statessuch as ESTABLISHED, TIME_WAIT, and FIN_WAIT. These connection states are highly valuable for threat hunting and network analysis. During DDoS activity-especially reflected or amplification-style attacks, or when a server is abused as part of an attack-connections often remain half- open, rapidly transition to TIME_WAIT, or fail to fully establish. In contrast, legitimate web traffic typically results in stable, short-lived ESTABLISHED sessions that follow predictable patterns.
Option B (destination port) is not useful here because most web traffic-both legitimate and malicious- commonly uses ports 80 or 443. Option C (IP address of the web server) provides no filtering value because all traffic already originates from that server. Option D (protocol) is also ineffective, as both normal and DDoS traffic in this case use TCP.
From a professional SOC and threat hunting standpoint,connection state analysisis a foundational technique for detecting volumetric attacks, beaconing behavior, and abnormal session churn. By filtering logs based on connection status, analysts can quickly isolate suspicious patterns such as excessive short-lived connections, abnormal teardown behavior, or asymmetric session states that are characteristic of DDoS-related activity.
This approach aligns with mature threat hunting practices:when indicators overlap, pivot to behavioral attributes. Connection status provides the necessary behavioral signal to separate expected traffic from attack traffic and supports faster, more accurate incident response.

NEW QUESTION # 133
What is the purpose of proactively conducting threat hunting in a cybersecurity environment?

- A. To detect and neutralize threats that have bypassed traditional security measures.
- B. To install new antivirus software on all devices.
- C. To generate automated cybersecurity reports.
- D. To respond to security incidents after they have already occurred.

Answer: A

NEW QUESTION # 134
Which of the following is NOT a common outcome of threat hunting?

- A. Identification of unknown threats
- B. Reduction of false positives
- C. Increased performance of network devices
- D. Improved security posture

Answer: C

NEW QUESTION # 135
.....

Although the passing rate of our 300-220 simulating exam is nearly 100%, we can refund money in full if you are still worried that you may not pass. You don't need to worry about the complexity of the refund process at all, we've made it quite simple. As long as you provide us with proof that you failed the exam after using our 300-220, we can refund immediately. If you encounter any problems during the refund process, you can also contact our customer service staff at any time. They will help you solve the problem as quickly as possible. That is to say, our 300-220 Exam Questions almost guarantee that you pass the exam. Even if you don't pass, you don't have to pay any price for our 300-220 simulating exam. I hope we have enough sincerity to impress you.

www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest It-Tests 300-220 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1eriICE1gL6nBDSjtRSAxW6FwuhPrJ8xY