CISCO 300-220 STUDY GUIDE PDF

Cisco CyberOps Professional Certification Questions & Answers

Details of the Exam-Syllabus-Questions

300-220

Cisco Certified Specialist Threat Hunting and Defending

55-65 Questions Exam – Variable (750-850 / 1000 Approx.) Cut Score – Duration of 90 minutes

Table of Contents:

Get an Overview of the 300-220 Certification:

Who should take the **300-220 exam**? This is the first question that comes to a candidate's mind when preparing for the CyberOps Professional certification. The 300-220 certification is suitable for candidates who are keen to earn knowledge on the CyberOps and grab their Cisco Certified Specialist Threat Hunting and Defending. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But 300-220 study guide PDF is here to solve the problem. 300-220 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the Cisco 300-220 Certification?

There are several reasons why one should grab the 300-220 certification.

- The CyberOps Professional certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the **Cisco Certified Specialist Threat Hunting and Defending** is a powerful qualification for a prosperous career.

What Is the Cisco 300-220 CyberOps Professional Certification Exam Structure?

Exam Name	Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps
Exam Number	300-220 CBRTHD
Exam Price	$300 USD
Duration	90 minutes
Number of Questions	55-65
Passing Score	Variable (750-850 / 1000 Approx.)
Recommended Training	**Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD)**

Exam Registration	PEARSON VUE
Sample Questions	Cisco 300-220 Sample Questions
Practice Exam	Cisco Certified Specialist Threat Hunting and Defending Practice Test

Enhance Knowledge with 300-220 Sample Questions:

Question: 1

What indicates a successful C2 communication detection using endpoint logs? (Choose two)

a) Increased outbound traffic to unknown IPs
b) Frequent system reboots
c) Unusual process tree formations
d) High volume of encrypted data sent to known ports

Answer: a, c

Question: 2

Endpoint artifacts are crucial for uncovering undetected threats. Which of the following are considered endpoint artifacts? (Choose two)

a) Router configuration files
b) Windows Registry keys
c) Bash history in Linux
d) DNS server logs

Answer: b, c

Question: 3

The integration of which products would most enhance analytical capabilities for threat hunting?

a) Standalone antivirus solutions
b) Disconnected SIEM and endpoint detection and response (EDR) platforms
c) SIEM, EDR, and threat intelligence platforms
d) Uncoordinated firewall and intrusion prevention systems

Answer: c

Question: 4

How can logs help in identifying the tactics, techniques, and procedures of a threat actor?

a) By showing the time of day attacks are most likely to occur
b) By revealing patterns and anomalies that indicate malicious activity
c) By indicating the level of user satisfaction with IT services
d) By tracking the number of successful phishing attempts

Answer: b

Question: 5

Detection tools are limited in their effectiveness due to: (Choose two)

a) The dynamic nature of cyber threats
b) The physical security of the data center
c) Encryption used by network protocols
d) The evolving tactics of threat actors

Answer: a, d

Question: 6

Changes to a detection methodology to augment analytical and process gaps might include: (Choose two)

a) Decreasing the use of automation and machine learning
b) Integrating threat intelligence feeds
c) Implementing behavioral analysis techniques
d) Relying solely on signature-based detection

Answer: b, c

Question: 7

_____ involves proactively searching through networks to detect and isolate advanced threats that evade existing security solutions.

a) Compliance auditing
b) Network optimization
c) Threat hunting
d) Software development

Answer: c

Question: 8

Which level of the Pyramid of Pain is most difficult for attackers to change and adapt to when detected?

a) Hash values
b) IP addresses
c) Domain names
d) TTPs (Tactics, Techniques, and Procedures)

Answer: d

Question: 9

When using the MITRE ATT&CK framework to model threats, changes in _____ are critical for understanding evolving attack strategies.

a) tactics, techniques, and procedures
b) encryption algorithms
c) software development methodologies
d) organizational policies

Answer: a

Question: 10

A comprehensive playbook addresses which phases of incident response?

(Choose two)

a) Detection
b) Budget planning
c) Recovery
d) Lunch break scheduling

Answer: a, c

What Study Guide Works Best in Acing the Cisco 300-220 CyberOps Professional Certification?

The 300-220 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the CyberOps Professional exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the Cisco 300-220 training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and Utilize the Cisco 300-220 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform

well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, 300-220 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven 300-220 Practice Test for Success!!!

Do you want to pass the 300-220 exam on your first attempt? Stop worrying; we, NWExam.com are here to provide you the best experience during your Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **300-220 practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.