CISCO 300-220

Cisco CyberOps Professional Certification Questions & Answers

Exam Summary – 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:

Know Your 300-220 Certification Well:

The 300-220 is best suitable for candidates who want to gain knowledge in the Cisco CyberOps. Before you start your 300-220 preparation you may struggle to get all the crucial CyberOps Professional materials like 300-220 syllabus, sample questions, study guide.

But don't worry the 300-220 PDF is here to help you prepare in a stress-free manner.
The PDF is a combination of all **your queries like**-

- What is in the 300-220 syllabus?
- How many questions are there in the 300-220 exam?
- Which Practice test would help me to pass the 300-220 exam at the first attempt?

Passing the 300-220 exam makes you Cisco Certified Specialist Threat Hunting and Defending. Having the CyberOps Professional certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Cisco 300-220 CyberOps Professional Certification Details:

Exam Name	Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps
Exam Code	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**

300-220 Syllabus:

Section	Weight	Objectives
Threat Hunting Fundamentals	20%	- Apply the Threat Hunting Maturity Model to an organization's environment, as it relates to the Pyramid of Pain - Describe threats and how to model them with standards such as MITRE ATT&CK, MITRE CAPEC, TaHiTI, and PASTA - Describe the limiting factors of detection tools for malware behavior, propagation, and detection - Describe the advantages and disadvantages of automation (such as artificial intelligence and machine learning) in the operation of a SOC - Determine differences in tactics, techniques, and procedures of an advanced persistent threat and threat actor using logs - Interpret a threat intelligence report and draw conclusions about a threat actor (known advanced persistent threat/commodity human-driven/commodity machine-driven) • tactics • techniques • procedures
Threat Modeling Techniques	10%	- Select the threat modeling approach for a given scenario - Use MITRE ATT&CK to model threats (tactics, techniques, and procedures or changes in tactics, techniques, and procedures) - Describe the uses of structured and unstructured threat hunting - Determine the priority level of attacks based on the Cyber Kill Chain and MITRE ATT&CK - Determine the priority level of attacks based on the MITRE CAPEC model - Perform threat intelligence handling: gathering, cataloging, utilizing, and removing

Section	Weight	Objectives
Threat Actor Attribution Techniques	20%	- Determine attack tactics, techniques, and procedures using logs - Interpret tactics, techniques and procedures of a given threat actor - Select the delivery method, payload, tactic, or timeline that indicates an authorized assessment or an attack (threat actor or penetration tester) - Determine usable artifacts for detection of advanced persistent threat actors at all levels of the Pyramid of Pain • tactics • techniques • procedures
Threat Hunting Techniques	20%	- Use scripting languages (such as Python and PowerShell) to augment detection or analytics - Perform a cloud-native threat hunt - Determine undetected threats using endpoint artifacts - Determine the C2 communications to and from infected hosts using endpoint applications, processes, and logs - Select suspicious activity using session and protocol data - Determine the stage of infection within C2 communications using traffic data - Select weakness in code using code-level analysis tools (such as PE Checker, BURP Suite, and SEM Grep) - Describe the analysis process for applications and operating systems used by IoT devices - Describe memory-resident attacks and how to perform analysis using memory-specific tools (such as Volatility) - Construct a signature for detection or analysis - Recognize the likelihood of attack by an attack vector within a given environment
Threat Hunting Processes	20%	- Describe the process to identify memory-resident attacks - Determine compromises by reverse engineering - Determine known and unknown gaps in detection • vulnerabilities • configuration errors • threats

Section	Weight	Objectives
		- Interpret data from memory-specific tools - Construct a runbook or playbook to address a detectable scenario - Recommend tools, configurations, detection, and deception techniques for a given scenario - Recommend attack remediation strategies based on the results of a threat assessment - Recommend changes to improve the effectiveness and efficiency of a threat hunt - Recommend security countermeasures and mitigations for identified risks
Threat Hunting Outcomes	10%	- Describe how multiproduct integration enhances data visibility within a product and accelerates analysis - Diagnose analytical gaps using threat hunting methodologies - Recommend a mitigation strategy to block C2 traffic - Recommend changes in hunt capability to advance to the next Threat Hunting Maturity Model phase - Recommend changes to a detection methodology to augment analytical and process gaps - Use presentation resources to convey findings and direct environmental change

Cisco 300-220 Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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: 5

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: 6

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

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

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: 9

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: 10

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

Study Guide to Crack Cisco CyberOps Professional 300-220 Exam:

- Getting details of the 300-220 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 300-220 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Cisco provided training for 300-220 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 300-220 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 300-220 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for 300-220 Certification

Make NWExam.com your best friend during your Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps exam preparation. We provide authentic practice tests for the 300-220 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual 300-220 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the 300-220 exam.

Start Online practice of 300-220 Exam by visiting URL
https://www.nwexam.com/cisco/300-220-conducting-threat-hunting-and-defending-using-cisco-technologies-cyberops-cbrthd