CISCO 350-201

Cisco SP Optical Technology Field Engineer Representative Certification Questions & Answers

Exam Summary – Syllabus – Questions

350-201

[Cisco Certified CyberOps Specialist - CyberOps Core]

90-110 Questions Exam – Variable (750-850 / 1000 Approx.) Cut Score – Duration of 120 minutes

Table of Contents:

Know Your 350-201 Certification Well:

The 350-201 is best suitable for candidates who want to gain knowledge in the Cisco CyberOps. Before you start your 350-201 preparation you may struggle to get all the crucial SP Optical Technology Field Engineer Representative materials like 350-201 syllabus, sample questions, study guide.

But don't worry the 350-201 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 350-201 syllabus?
- How many questions are there in the 350-201 exam?
- Which Practice test would help me to pass the 350-201 exam at the first attempt?

Passing the 350-201 exam makes you Cisco Certified CyberOps Specialist - CyberOps Core. Having the SP Optical Technology Field Engineer Representative 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 350-201 SP Optical Technology Field Engineer Representative Certification Details:

Exam Name	Performing CyberOps Using Cisco Security Technologies
Exam Code	350-201
Exam Price	$400 USD
Duration	120 minutes
Number of Questions	90-110
Passing Score	Variable (750-850 / 1000 Approx.)
Recommended Training	Performing CyberOps Using Cisco Security Technologies (CBRCOR) CBRCOR study materials
Exam Registration	PEARSON VUE
Sample Questions	Cisco 350-201 Sample Questions

Practice Exam	**Cisco Certified CyberOps Specialist - CyberOps Core Practice Test**

350-201 Syllabus:

Section	Weight	Objectives
Fundamentals	20%	- Interpret the components within a playbook - Determine the tools needed based on a playbook scenario - Apply the playbook for a common scenario (for example, unauthorized elevation of privilege, DoS and DDoS, website defacement) - Infer the industry for various compliance standards (for example, PCI, FISMA, FedRAMP, SOC, SOX, PCI, GDPR, Data Privacy, and ISO 27101) - Describe the concepts and limitations of cyber risk insurance - Analyze elements of a risk analysis (combination asset, vulnerability, and threat) - Apply the incident response workflow - Describe characteristics and areas of improvement using common incident response metrics - Describe types of cloud environments (for example, IaaS platform) - Compare security operations considerations of cloud platforms (for example, IaaS, PaaS)
Techniques	30%	- Recommend data analytic techniques to meet specific needs or answer specific questions - Describe the use of hardening machine images for deployment - Describe the process of evaluating the security posture of an asset - Evaluate the security controls of an environment, diagnose gaps, and recommend improvement - Determine resources for industry standards and recommendations for hardening of systems - Determine patching recommendations, given a scenario - Recommend services to disable, given a scenario - Apply segmentation to a network - Utilize network controls for network hardening - Determine SecDevOps recommendations (implications) - Describe use and concepts related to using a Threat Intelligence Platform (TIP) to automate intelligence - Apply threat intelligence using tools - Apply the concepts of data loss, data leakage, data in

Section	Weight	Objectives
		motion, data in use, and data at rest based on common standards - Describe the different mechanisms to detect and enforce data loss prevention techniques • host-based • network-based • application-based • cloud-based - Recommend tuning or adapting devices and software across rules, filters, and policies - Describe the concepts of security data management - Describe use and concepts of tools for security data analytics - Recommend workflow from the described issue through escalation and the automation needed for resolution - Apply dashboard data to communicate with technical, leadership, or executive stakeholders - Analyze anomalous user and entity behavior (UEBA) - Determine the next action based on user behavior alerts - Describe tools and their limitations for network analysis (for example, packet capture tools, traffic analysis tools, network log analysis tools) - Evaluate artifacts and streams in a packet capture file - Troubleshoot existing detection rules - Determine the tactics, techniques, and procedures (TTPs) from an attack
Processes	30%	- Prioritize components in a threat model - Determine the steps to investigate the common types of cases - Apply the concepts and sequence of steps in the malware analysis process: • Extract and identify samples for analysis (for example, from packet capture or packet analysis tools) • Perform reverse engineering • Perform dynamic malware analysis using a sandbox environment • Identify the need for additional static malware analysis

Section	Weight	Objectives
		• Perform static malware analysis • Summarize and share results - Interpret the sequence of events during an attack based on analysis of traffic patterns - Determine the steps to investigate potential endpoint intrusion across a variety of platform types (for example, desktop, laptop, IoT, mobile devices) - Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs), given a scenario - Determine IOCs in a sandbox environment (includes generating complex indicators) - Determine the steps to investigate potential data loss from a variety of vectors of modality (for example, cloud, endpoint, server, databases, application), given a scenario - Recommend the general mitigation steps to address vulnerability issues - Recommend the next steps for vulnerability triage and risk analysis using industry scoring systems (for example, CVSS) and other techniques
Automation	20%	- Compare concepts, platforms, and mechanisms of orchestration and automation - Interpret basic scripts (for example, Python) - Modify a provided script to automate a security operations task - Recognize common data formats (for example, JSON, HTML, CSV, XML) - Determine opportunities for automation and orchestration - Determine the constraints when consuming APIs (for example, rate limited, timeouts, and payload) - Explain the common HTTP response codes associated with REST APIs - Evaluate the parts of an HTTP response (response code, headers, body) - Interpret API authentication mechanisms: basic, custom token, and API keys - Utilize Bash commands (file management, directory navigation, and environmental variables) - Describe components of a CI/CD pipeline - Apply the principles of DevOps practices - Describe the principles of Infrastructure as Code

Cisco 350-201 Sample Questions:

Question: 1

The physical security department received a report that an unauthorized person followed an authorized individual to enter a secured premise. The incident was documented and given to a security specialist to analyze. Which step should be taken at this stage?

a) Determine the assets to which the attacker has access
b) Identify assets the attacker handled or acquired
c) Change access controls to high risk assets in the enterprise
d) Identify movement of the attacker in the enterprise

Answer: d

Question: 2

How is a SIEM tool used?

a) To collect security data from authentication failures and cyber attacks and forward it for analysis
b) To search and compare security data against acceptance standards and generate reports for analysis
c) To compare security alerts against configured scenarios and trigger system responses
d) To collect and analyze security data from network devices and servers and produce alerts

Answer: d

Question: 3

Employees report computer system crashes within the same week. An analyst is investigating one of the computers that crashed and discovers multiple shortcuts in the system's startup folder. It appears that the shortcuts redirect users to malicious URLs.

What is the next step the engineer should take to investigate this case?

a) Remove the shortcut files
b) Check the audit logs
c) Identify affected systems
d) Investigate the malicious URLs

Answer: c

Question: 4

Where do threat intelligence tools search for data to identify potential malicious IP addresses, domain names, and URLs?

a) Internet
b) internal database
c) internal cloud
d) customer data

Answer: a

Question: 5

What do 2xx HTTP response codes indicate for REST APIs?

a) additional action must be taken by the client to complete the request
b) the server takes responsibility for error status codes
c) successful acceptance of the client's request
d) communication of transfer protocol-level information

Answer: c

Question: 6

How does Wireshark decrypt TLS network traffic?

a) with a key log file using per-session secrets
b) using an RSA public key
c) by observing DH key exchange
d) by defining a user-specified decode-as

Answer: a

Question: 7

Which command does an engineer use to set read/write/execute access on a folder for everyone who reaches the resource?

a) chmod 666
b) chmod 777
c) chmod 775
d) chmod 774

Answer: b

Question: 8

According to GDPR, what should be done with data to ensure its confidentiality, integrity, and availability?

a) Perform a vulnerability assessment
b) Conduct a data protection impact assessment
c) Conduct penetration testing
d) Perform awareness testing

Answer: b

Question: 9

The incident response team receives information about the abnormal behavior of a host. A malicious file is found being executed from an external USB flash drive. The team collects and documents all the necessary evidence from the computing resource. What is the next step?

a) Conduct a risk assessment of systems and applications
b) Isolate the infected host from the rest of the subnet
c) Install malware prevention software on the host
d) Analyze network traffic on the host's subnet

Answer: b

Question: 10

What is needed to assess risk mitigation effectiveness in an organization?

a) cost-effectiveness of control measures
b) analysis of key performance indicators
c) compliance with security standards
d) updated list of vulnerable systems

Answer: a

Study Guide to Crack Cisco SP Optical Technology Field Engineer Representative 350-201 Exam:

- Getting details of the 350-201 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 350-201 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 350-201 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 350-201 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 350-201 practice tests is must. Continuous practice will make you an expert in all syllabus areas.