FIREFLY

CISCO PARTNER Platinum Learning

Performing Cyberops Using Cisco Security Technologies • CBRCOR

DURATION: 5 DAYS | **PRICE:** USD 3995 | **CLCs:** 40 | **CE:** 40

COURSE CODE: CBRCOR | **FORMAT:** Lecture & Lab

COURSE DESCRIPTION

The Performing Cybersecurity Using Cisco Security Technologies (CBRCOR) training guides you through cybersecurity operations fundamentals, methods, and automation. The knowledge you gain in this training will prepare you for the role of Information Security Analyst on a Security Operations Center (SOC) team. You will learn foundational concepts and their application in real-world scenarios, and how to leverage playbooks in formulating an Incident Response (IR). The training teaches you how to use automation for security using cloud platforms and a SecDevOps methodology. You will learn the techniques for detecting cyberattacks, analyzing threats, and making appropriate recommendations to improve cybersecurity.

This training prepares you for the 350-201 CBRCOR v1.2 exam. If passed, you earn the Cisco Certified Specialist – Cybersecurity Core certification and satisfy the core exam requirement for the Cisco Certified Cybersecurity Professional certification.

HOW YOU'LL BENEFIT

This training will help you:

- Develop essential cybersecurity skills in SOC operations, threat detection, and incident response through real-world labs and scenarios
- Gain hands-on experience with leading security tools such as Cisco XDR, Splunk Phantom, and Firepower NGFW
- Learn automation and SecDevOps practices to improve efficiency and effectiveness in security operations
- Prepare for the 350-201 CBRCOR v1.2 exam
- Earn 40 CE credits toward recertification

WHO SHOULD ENROLL

- Cybersecurity Engineers
- Cybersecurity Investigators
- Incident Managers
- Incident Responders
- Network Engineers
- SOC Analysts currently functioning at entry level with a minimum of 1 year of experience

Performing Cyberops Using Cisco Security Technologies • CBRCOR

WHAT TO EXPECT IN THE EXAM

Performing Cybersecurity Using Cisco Security Technologies (350-201 CBRCOR) v1.2 is a 120-minute exam associated with the Cisco Certified Specialist – Cybersecurity Core certification and satisfies the core exam requirement for the Cisco Certified Cybersecurity Professional certification.

This exam tests your knowledge of core cybersecurity operations, including:

- Cybersecurity fundamentals
- Techniques
- Processes
- Automation

COURSE OBJECTIVES

- Describe the types of service coverage within a SOC and operational responsibilities associated with each
- Compare security operations considerations of cloud platforms
- Describe the general methodologies of SOC platforms development, management, and automation
- Describe asset segmentation, segregation, network segmentation, microsegmentation, and approaches to each, as part of asset controls and protections
- Describe Zero Trust and associated approaches, as part of asset controls and protections
- Perform incident investigations using Security Information and Event Management (SIEM) and/or security orchestration and automation (SOAR) in the SOC
- Use different types of core security technology platforms for security monitoring, investigation, and response
- Describe the DevOps and SecDevOps processes
- Describe the common data formats (e.g., JavaScript Object Notation (JSON), HTML, XML, and Comma-Separated Values (CSV))
- Describe API authentication mechanisms
- Analyze the approach and strategies of threat detection, during monitoring, investigation, and response
- Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs)
- Interpret the sequence of events during an attack based on analysis of traffic patterns
- Describe the different security tools and their limitations for network analysis (e.g., packet capture tools, traffic analysis tools, and network log analysis tools)
- Analyze anomalous user and entity behavior (UEBA)
- Perform proactive threat hunting following best practices

COURSE PREREQUISITES

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- Familiarity with UNIX/Linux shells (bash, csh) and shell commands
- Familiarity with the Splunk search and navigation functions
- Basic understanding of scripting using one or more of Python, JavaScript, PHP or similar

These skills can be found in the following Cisco Learning Offerings:

- Understanding Cisco Cybersecurity

Performing Cyberops Using Cisco Security Technologies • CBRCOR

Operations Fundamentals (CBROPS)
• Implementing and Administering Cisco Solutions (CCNA)

COURSE OUTLINE

• Understanding Risk Management and SOC Operations
• Understanding Analytical Processes and Playbooks
• Understanding Cloud Service Model Security Responsibilities
• Understanding Enterprise Environment Assets
• Understanding APIs
• Understanding SOC Development and Deployment Models
• Investigating Packet Captures, Logs, and Traffic Analysis
• Investigating Endpoint and Appliance Logs
• Implementing Threat Tuning
• Threat Research and Threat Intelligence Practices
• Performing Security Analytics and Reports in a SOC
• Malware Forensics Basics
• Threat Hunting Basics
• Performing Incident Investigation and Response

LAB OUTLINE

• Explore Cisco XDR
• Explore Splunk Phantom Playbooks
• Evaluate Assets in a Typical Enterprise Environment
• Fix a Python API Script
• Create Bash Basic Scripts
• Examine Cisco Firepower Packet Captures and PCAP Analysis
• Validate an Attack and Determine the Incident Response
• Submit a Sample to Cisco Secure Malware Analytics for Analysis
• Endpoint-Based Attack Scenario Referencing MITRE ATTACK®
• Explore Cisco Firepower NGFW Access Control Policy and Snort Rules
• Investigate IOCs using Cisco XDR
• Explore the ThreatConnect Threat Intelligence Platform
• Track the TTPs of a Successful Attack Using a TIP
• Reverse Engineer Malware
• Perform Threat Hunting
• Conduct an Incident Response

Instructor Led Training

To view the schedule and secure your site

SIGN UP HERE