Training overview
Cisco public

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Description

The **Performing CyberOps 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 v1.1 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. This training also earns you 40 Continuing Education (CE) credits toward recertification.

How you'll benefit

This training will help you:

- Gain an advanced understanding of the tasks involved for senior-level roles in a security operations center
- Configure common tools and platforms used by security operation teams via practical application
- Prepare you to respond like a hacker in real-life attack scenarios and submit recommendations to senior management
- Prepare for the 350-201 CBRCOR v1.1 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

Technology areas

- Cybersecurity

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
- Explain asset segmentation, segregation, network segmentation, micro-segmentation, 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
- Explain the common data formats, for example, JavaScript Object Notation (JSON), HTML, XML, 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 (for example, packet capture tools, traffic analysis tools, network log analysis tools)
- Analyze anomalous user and entity behavior (UEBA)
- Perform proactive threat hunting following best practices

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

Outline

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

Lab Outline

- Explore Cisco SecureX Orchestration
- Explore Splunk Phantom Playbooks
- Examine Cisco Firepower Packet Captures and PCAP Analysis
- Validate an Attack and Determine the Incident Response
- Submit a Malicious File to Cisco Threat Grid for Analysis
- Endpoint-Based Attack Scenario Referencing MITRE ATTACK
- Evaluate Assets in a Typical Enterprise Environment
- Explore Cisco Firepower NGFW Access Control Policy and Snort Rules
- Investigate IOCs from Cisco Talos Blog Using Cisco SecureX
- Explore the ThreatConnect Threat Intelligence Platform
- Track the TTPs of a Successful Attack Using a TIP
- Query Cisco Umbrella Using Postman API Client
- Fix a Python API Script
- Create Bash Basic Scripts
- Reverse Engineer Malware
- Perform Threat Hunting
- Conduct an Incident Response

What to expect on the exam

Performing Cybersecurity Using Cisco Security Technologies (350-201 CBRCOR) v1.1 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

Links

- Cisco U. Learning Path
- Cisco Learning Network Store
- Cisco Learning Locator