



Performing CyberOps Using Cisco Security Technologies (CBRCOR)

***WHERE GREAT TRAINING
HAPPENS EVERYDAY!***



Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Course Duration

5 Days

Course Price

\$4,295.00

40 CLCs

Methods of Delivery

In-Person ILT

Virtual ILT

Onsite ILT

About this Class

In this Performing Cybersecurity Using Cisco Security Technologies course provides a comprehensive introduction to modern Security Operations Center practices, focusing on how security teams detect, analyze, investigate, and respond to cyber threats across enterprise and cloud environments. It is designed for SOC analysts, security engineers, and incident responders who need to understand the full security operations lifecycle, from risk management and detection to investigation, threat hunting, and response. The course emphasizes structured analytical processes, repeatable playbooks, and hands-on investigation techniques. Students begin by exploring risk management concepts, SOC operations, analytical workflows, and playbooks, establishing a foundation for effective security monitoring and decision-making. The curriculum then examines enterprise assets, cloud security responsibility models, APIs, and SOC deployment models to provide context for security operations. Technical investigation skills are developed through packet capture analysis, network traffic inspection, and log analysis from endpoints and security appliances, with an emphasis on threat tuning to improve detection accuracy and reduce false positives.

Advanced topics include threat research, threat intelligence platforms, security analytics, malware forensics, and threat hunting fundamentals aligned with frameworks such as MITRE ATTACK®. The course culminates in incident investigation and response, where students validate attacks, analyze indicators of compromise, and execute structured response actions. Extensive hands-on labs using tools such as Cisco XDR, Cisco Firepower, Splunk Phantom, and threat intelligence platforms reinforce real-world SOC workflows, preparing learners to operate effectively in a modern, threat-centric SOC environment.

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

How you will benefit

This class 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

Why Attend with Current Technologies CLC

- Our Instructors are the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The job roles best suited to the material in this course are:

- Cybersecurity engineer
- Cybersecurity investigator
- Incident manager
- Incident responder
- Network engineer
- SOC analysts currently functioning at entry level with a minimum of 1 year of experience

Prerequisites

To fully benefit from this course, you should have the following knowledge and skills:

- 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.

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Objectives

After taking this course, you should be able to:

- 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

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Course Outline

Module 1: Understanding Risk Management and SOC Operations

Module 2: Understanding Analytical Processes and Playbooks

Module 3: Understanding Cloud Service Model Security Responsibilities

Module 4: Understanding Enterprise Environment Assets

Module 5: Understanding APIs

Module 6: Understanding SOC Development and Deployment Models

Module 7: Investigating Packet Captures, Logs, and Traffic Analysis

Module 8: Investigating Endpoint and Appliance Logs

Module 9: Implementing Threat Tuning

Module 10: Threat Research and Threat Intelligence Practices

Module 11: Performing Security Analytics and Reports in a SOC

Module 12: Malware Forensics Basics

Module 13: Threat Hunting Basics

Module 14: Performing Incident Investigation and Response

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Lab Outline

- Lab 1: Explore Cisco XDR
- Lab 2: Explore Splunk Phantom Playbooks
- Lab 3: Evaluate Assets in a Typical Enterprise Environment
- Lab 4: Fix a Python API Script
- Lab 5: Create Bash Basic Scripts
- Lab 6: Examine Cisco Firepower Packet Captures and PCAP Analysis
- Lab 7: Validate an Attack and Determine the Incident Response
- Lab 8: Submit a Sample to Cisco Secure Malware Analytics for Analysis
- Lab 9: Endpoint-Based Attack Scenario Referencing MITRE ATTACK®
- Lab 10: Explore Cisco Firepower NGFW Access Control Policy and Snort Rules
- Lab 11: Investigate IOCs using Cisco XDR
- Lab 12: Explore the ThreatConnect Threat Intelligence Platform
- Lab 13: Track the TTPs of a Successful Attack Using a TIP
- Lab 14: Reverse Engineer Malware
- Lab 15: Perform Threat Hunting
- Lab 16: Conduct an Incident Response