CBRCOR - PERFORMING CYBEROPS USING CISCO SECURITY TECHNOLOGIES V1.0

Course Code: 821350

The Performing CyberOps Using Cisco Security Technologies (CBRCOR) course guides you through cybersecurity operations fundamentals, methods, and automation. The knowledge you gain in this course 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 course 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 course also earns you 40 Continuing Education (CE) credits towards recertification and prepares you for the 350-201 CBRCOR core exam.

What You'll Learn

Upon successful completion of 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.
- 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.

Who Needs to Attend

Cybersecurity analysts, engineers, investigators and incident responders.

Prerequisites

Attendees should meet the following pre-requisites:
- 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.

Recommended prerequisites:

CBRCOR - PERFORMING CYBEROPS USING CISCO SECURITY TECHNOLOGIES V1.0

Course Code: 821350

CLASSROOM LIVE	$3,995 USD	5 Day

Classroom Live 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

Classroom Live Labs

- 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

CBRCOR - PERFORMING CYBEROPS USING CISCO SECURITY TECHNOLOGIES V1.0

Course Code: 821350

VIRTUAL CLASSROOM LIVE	$3,995 USD	5 Day

Virtual Classroom Live 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

Virtual Classroom Live Labs

- 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

Oct 6 - 10, 2025 | 8:30 AM - 4:30 PM EDT

Jan 12 - 16, 2026 | 8:30 AM - 4:30 PM EST

Apr 20 - 24, 2026 | 8:30 AM - 4:30 PM EDT

CBRCOR - PERFORMING CYBEROPS USING CISCO SECURITY TECHNOLOGIES V1.0

Course Code: 821350

ON-DEMAND	$1,000 USD

On-Demand 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

On-Demand Labs

- 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

CBRCOR - PERFORMING CYBEROPS USING CISCO SECURITY TECHNOLOGIES V1.0

Course Code: 821350

PRIVATE GROUP TRAINING	5 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.