CBRCOR - PERFORMING CYBEROPS USING CISCO SECURITY TECHNOLOGIES

Course Code: 821350

350-201 Performing CyberOps Using Cisco Security Technologies (CBRCOR) is a 120-minute exam associated with the Cisco CyberOps Professional Certification. The multiple-choice format tests knowledge of core cybersecurity operations including cybersecurity fundamentals, techniques, policies, processes, and automation

The exam will test for knowledge in the following areas:

- Monitoring for cyberattacks
- Analyzing high volume of data using automation tools and platforms—both open source and commercial
- Accurately identifying the nature of attack and formulate a mitigation plan
- Scenario-based questions; for example, using a screenshot of output from a tool, you may be asked to interpret portions of output and establish conclusions

This course is eligible for 40 Continuing Education Credits (ILT & ELT Modality).

What You'll Learn

This course 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 core exam
- Earn 30 CE credits toward recertification

Who Needs to Attend

- 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

Although there are no mandatory prerequisites, to fully benefit from this course, you should have the following knowledge:

- 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.

CBRCOR - PERFORMING CYBEROPS USING CISCO SECURITY TECHNOLOGIES

Course Code: 821350

CLASSROOM LIVE	$4,195 USD	5 Day

CBRCOR - PERFORMING CYBEROPS USING CISCO SECURITY TECHNOLOGIES

Course Code: 821350

VIRTUAL CLASSROOM LIVE	$4,195 USD	5 Day

Virtual Classroom Live Outline

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.
- 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.

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

May 19 - 23, 2025 | 8:30 AM - 4:30 PM EDT

CBRCOR - PERFORMING CYBEROPS USING CISCO SECURITY TECHNOLOGIES

Course Code: 821350

ON-DEMAND	$1,000 USD

CBRCOR - PERFORMING CYBEROPS USING CISCO SECURITY TECHNOLOGIES

Course Code: 821350

PRIVATE GROUP TRAINING	5 Day

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

Date created: 3/29/2025 5:24:32 AM