Current Technologies
Computer Learning Centers

cisco Partner
Platinum Learning

Performing CyberOps Using Cisco Security Technologies (CBRCOR) V1.0

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Performing CyberOps Using Cisco Security Technologies (CBRCOR) V1.0

Course Duration

5 Days

Course Price

$4,295.00
40 CLCs

Methods of Delivery

In-Person ILT
Virtual ILT
Onsite ILT

About this Class

The Performing CyberOps Using Cisco Security Technologies (CBRCOR) V1.0 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.

Performing CyberOps Using Cisco Security Technologies (CBRCOR) V1.0

How you will benefit

This class 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 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) V1.0

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.
- 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.

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Performing CyberOps Using Cisco Security Technologies (CBRCOR) V1.0

Course Outline

Module 1: Understanding Risk Management and SOC Operations

Module 2: Understanding Analytical Processes and Playbooks

Module 3: Investigating Packet Captures, Logs, and Traffic Analysis

Module 4: Investigating Endpoint and Appliance Logs

Module 5: Understanding Cloud Service Model Security Responsibilities

Module 6: Understanding Enterprise Environment Assets

Module 7: Implementing Threat Tuning

Module 8: Threat Research and Threat Intelligence Practices

Module 9: Understanding APIs

Module 10: Understanding SOC Development and Deployment Models

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

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Performing CyberOps Using Cisco Security Technologies (CBRCOR) V1.0

Lab Outline

- Lab 1: Explore Cisco SecureX Orchestration
- Lab 2: Explore Splunk Phantom Playbooks
- Lab 3: Examine Cisco Firepower Packet Captures and PCAP Analysis
- Lab 4: Validate an Attack and Determine the Incident Response
- Lab 5: Submit a Malicious File to Cisco Threat Grid for Analysis
- Lab 6: Endpoint-Based Attack Scenario Referencing MITRE ATTACK
- Lab 7: Evaluate Assets in a Typical Enterprise Environment
- Lab 8: Explore Cisco Firepower NGFW Access Control Policy and Snort Rules
- Lab 9: Investigate IOCs from Cisco Talos Blog Using Cisco SecureX
- Lab 10: Explore the ThreatConnect Threat Intelligence Platform
- Lab 11: Track the TTPs of a Successful Attack Using a TIP
- Lab 12: Query Cisco Umbrella Using Postman API Client
- Lab 13: Fix a Python API Script
- Lab 14: Create Bash Basic Scripts
- Lab 15: Reverse Engineer Malware
- Lab 16: Perform Threat Hunting
- Lab 17: Conduct an Incident Response