Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

In this Understanding Cisco Cybersecurity Operations Fundamentals course provides a comprehensive introduction to Security Operations Center (SOC) concepts, workflows, and technologies, focusing on how security teams detect, analyze, and respond to cyber threats in modern enterprise and cloud environments. It is designed to build foundational knowledge across operating systems, networking, security monitoring, and incident response while emphasizing a threat-centric approach.

The course begins by defining the role of the SOC, key performance metrics, and operational workflows, including the use of automation to improve efficiency and response time. Learners gain foundational understanding of Windows and Linux operating systems, endpoint security technologies, network infrastructure, and network security monitoring tools, which are critical for effective threat detection and analysis.

Additional topics include common TCP/IP-based attacks, data type categories used in security analysis, basic cryptography concepts, and cloud security fundamentals with an emphasis on securing cloud deployments. The course then transitions into threat-centric SOC operations, covering incident analysis, common attack vectors, malicious activity identification, behavioral pattern recognition, threat hunting resources, and event correlation and normalization.

Hands-on labs reinforce these concepts by exploring operating systems, endpoint and network security tools, analyzing attack techniques, investigating suspicious DNS and browser-based activity, correlating logs, packet captures, and alerts, and conducting threat hunts using tools such as Security Onion. Advanced scenarios include investigating advanced persistent threats, applying SOC playbooks, and simulating integrations between Cisco XDR and Splunk Enterprise, preparing learners for real-world SOC operations and incident response.

How you'll benefit

This class will help you:

- Learn the fundamental skills, techniques, technologies, and the hands-on practice necessary to prevent and defend against cyberattacks as part of a SOC team
- Prepare for the 200-201 CBROPS v1.2 exam
- Earn 30 CE credits toward recertification

Why Attend with Current Technologies CLC

- Our Instructors are in 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 primary audience for this course is as follows:

- Students pursuing a technical degree
- Current IT professionals
- Recent college graduates with a technical degree

Course Duration

5 days

Course Price

$4,295.00 or 43 CLCs

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

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 Ethernet and TCP/IP networking
- Working knowledge of the Windows and Linux operating systems
- Familiarity with basics of networking security concepts

OUTLINE

Module 1: Defining the Security Operations Center

Module 2: Understanding SOC Metrics

Module 3: SOC Workflow and Automation

Module 4: Windows Operating System Basics

Module 5: Understanding Linux Operating System Basics

Module 6: Understanding Endpoint Security Technologies

Module 7: Understanding Network Infrastructure and Network Security Monitoring Tools

Module 8: Understanding Common TCP/IP Attacks

Module 9: Exploring Data Type Categories

Module 10: Understanding Basic Cryptography Concepts

Module 11: Cloud Security Fundamentals

Module 12: Securing Cloud Deployments

Module 13: Understanding Incident Analysis in a Threat-Centric SOC

Module 14: Identifying Common Attack Vectors

Module 15: Identifying Malicious Activity

Module 16: Identifying Patterns of Suspicious Behavior

Module 17: Identifying Resources for Hunting Cyber Threats

Module 18: Understanding Event Correlation and Normalization

Module 19: Conducting Security Incident Investigations

Module 20: Using a Playbook Model to Organize Security Monitoring

Module 21: Describing Incident Response

LAB OUTLINE

- Lab 1: Explore the Windows Operating System
- Lab 2: Explore the Linux Operating System
- Lab 3: Explore Endpoint Security
- Lab 4: Explore TCP/IP Attacks
- Lab 5: Use NSM Tools to Analyze Data Categories
- Lab 6: Explore Cryptographic Technologies
- Lab 7: Investigate Hacker Methodology
- Lab 8: Investigate Browser-Based Attacks
- Lab 9: Analyze Suspicious DNS Activity
- Lab 10: Explore Security Data for Analysis
- Lab 11: Investigate Suspicious Activity Using Security Onion
- Lab 12: Hunt Malicious Traffic
- Lab 13: Cisco XDR to Splunk Enterprise Integration Simulation
- Lab 14: Correlate Event Logs, PCAPs, and Alerts of an Attack
- Lab 15: Investigate Advanced Persistent Threats
- Lab 16: Explore SOC Playbooks