UNDERSTANDING CISCO CYBERSECURITY OPERATIONS FUNDAMENTALS (CBROPS) V1.0

UNDERSTANDING CISCO CYBERSECURITY OPERATIONS FUNDAMENTALS (CBROPS) V1.0

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.1 training teaches you security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. This training teaches you how to monitor alerts and breaches, and how to understand and follow established procedures for response to alerts converted to incidents. Through a combination of lecture, hands-on labs, and self-study, you will learn the essential skills, concepts, and technologies to be a contributing member of a Cybersecurity Operations Center (SOC) including understanding the IT infrastructure, operations, and vulnerabilities.

This training helps you prepare for the Cisco® Certified CyberOps Associate certification and the role of a Junior or Entry-level cybersecurity operations analyst in a SOC. This training also earns you 30 Continuing Education (CE) credits towards recertification.

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 Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) exam which earns the Cisco Certified CyberOps Associate certification

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

OUTLINE

Module 1: Defining the Security Operations Center

Module 2: Understanding Network Infrastructure and Network Security Monitoring Tools

Module 3: Exploring Data Type Categories

Module 4: Understanding Basic Cryptography Concepts

Module 5: Understanding Common TCP/IP Attacks

Module 6: Understanding Endpoint Security Technologies

Module 7: Understanding Incident Analysis in a Threat-Centric SOC

Module 8: Identifying Resources for Hunting Cyber Threats

Module 9: Understanding Event Correlation and Normalization

Module 10: Identifying Common Attack Vectors

Module 11: Identifying Malicious Activity

Module 12: Identifying Patterns of Suspicious Behavior

Module 13: Conducting Security Incident Investigations

Module 14: Using a Playbook Model to Organize Security Monitoring

Module 15: Understanding SOC Metrics

Module 16: Understanding SOC Workflow and Automation

Module 17: Describing Incident Response

Module 18: Understanding the Use of VERIS

Module 19: Understanding Windows Operating System Basics

Module 20: Understanding Linux Operating System Basics

LAB OUTLINE

- **Lab 1: Use NSM Tools to Analyze Data Categories**
- **Lab 2: Explore Cryptographic Technologies**
- **Lab 3: Explore TCP/IP Attacks**
- **Lab 4: Explore Endpoint Security**
- **Lab 5: Investigate Hacker Methodology**
- **Lab 6: Hunt Malicious Traffic**
- **Lab 7: Correlate Event Logs, Packet Captures (PCAPs), and Alerts of an Attack**
- **Lab 8: Investigate Browser-Based Attacks**
- **Lab 9: Analyze Suspicious Domain Name System (DNS) Activity**

- **Lab 10: Explore Security Data for Analysis**
- **Lab 11: Investigate Suspicious Activity Using Security Onion**
- **Lab 12: Investigate Advanced Persistent Threats**
- **Lab 13: Explore SOC Playbooks**
- **Lab 14: Explore the Windows Operating System**
- **Lab 15: Explore the Linux Operating System**