Cisco Certified CyberOps Professional (CBROPS)

Price	Duration	Delivery Methods
$1,995.00	5 Daytime Classes Or 10 Evening Classes	Virtual, In-Person, Private Group,

CAREER SKILLS+™

The Understanding Cybersecurity Operations Fundamentals (CBROPS) v1.0 course teaches an understanding of the network infrastructure devices, operations, and vulnerabilities of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. You will learn basic information about security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data used to investigate security incidents. After completing this course, you will have the basic knowledge required to perform the job role of an associate-level cybersecurity analyst in a threat-centric security operations center to strengthen network protocol, protect your devices and increase operational efficiency. This course prepares you for the Cisco Certified CyberOps Associate certification. New – Recommended as preparation for the following exams: 200-201 - CBROPS Understanding Cisco Cybersecurity Operations Fundamentals Please note that this course is a combination of Instructor-Led and Self-Paced Study - 5 days in the classroom and approx. 1 day of self-study. The self-study content will be provided as part of the digital courseware that you will receive at the beginning of the course and should be part of your preparation for the exam.

Who Should Attend

This course is designed for an associate-level cybersecurity analyst who is working in security operation centers.

Course Objectives

Explain how a SOC operates and describe the different types of services that are performed from a Tier 1 SOC analyst’s perspective.

Explain Network Security Monitoring (NSM) tools that are available to the network security analyst.

Explain the data that is available to the network security analyst.

Describe the basic concepts and uses of cryptography.

Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts.

Understand common endpoint security technologies.

Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors.

Identify resources for hunting cyber threats.

Explain the need for event data normalization and event correlation.

Identify the common attack vectors.

Identify malicious activities.

Identify patterns of suspicious behaviors.

Conduct security incident investigations.

Explain the use of a typical playbook in the SOC.

Explain the use of SOC metrics to measure the effectiveness of the SOC.

Explain the use of a workflow management system and automation to improve the effectiveness of the SOC.

Describe a typical incident response plan and the functions of a typical CSIRT.

Explain the use of VERIS to document security incidents in a standard format.

Describe the Windows operating system features and functionality.

Describe the Linux operating system features and functionality.

Course Prerequisites

Skills and knowledge equivalent to those learned in Implementing and Administering Cisco Solutions (CCNA) course

Familiarity with Ethernet and TCP/IP networking

Working knowledge of the Windows and Linux operating systems

Familiarity with basics of networking security concepts

Agenda

1. Lessons

- Defining the Security Operations Center
- Understanding Network Infrastructure and Network Security Monitoring Tools
- Exploring Data Type Categories
- Understanding Basic Cryptography Concepts
- Understanding Common TCP/IP Attacks
- Understanding Endpoint Security Technologies
- Understanding Incident Analysis in a Threat-Centric SOC
- Identifying Resources for Hunting Cyber Threats
- Understanding Event Correlation and Normalization
- Identifying Common Attack Vectors
- Identifying Malicious Activity
- Identifying Patterns of Suspicious Behavior
- Conducting Security Incident Investigations
- Using a Playbook Model to Organize Security Monitoring
- Understanding SOC Metrics
- Understanding SOC Workflow and Automation
- Describing Incident Response
- Understanding the Use of VERIS
- Understanding Windows Operating System Basics
- Understanding Linux Operating System Basics

2. Lab Outline

- Configure the Initial Collaboration Lab Environment
- Use NSM Tools to Analyze Data Categories
- Explore Cryptographic Technologies
- Explore TCP/IP Attacks
- Explore Endpoint Security
- Investigate Hacker Methodology
- Hunt Malicious Traffic
- Correlate Event Logs, PCAPs, and Alerts of an Attack
- Investigate Browser-Based Attacks
- Analyze Suspicious DNS Activity
- Explore Security Data for Analysis
- Investigate Suspicious Activity Using Security Onion
- Investigate Advanced Persistent Threats
- Explore SOC Playbooks
- Explore the Windows Operating System
- Explore the Linux Operating System