

Understanding Cisco Cybersecurity Operations Fundamentals v1.0 (CBROPS) Training

Cisco Authorized Training · Applied Technology Academy

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0 course teaches you security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. This course teaches you how to monitor alerts and breaches, and how to understand and follow established procedures for response to alerts converted to incidents.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	5 Days	1 year: CBROPS	\$89,246	Yes

Course Overview

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 course 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.

After taking this course, you should be able to:

Explain how a Security Operations Center (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 Computer Security Incident Response Team (CSIRT).

Explain the use of Vocabulary for Event Recording and Incident Sharing (VERIS) to document security incidents in a standard format.

Course Outline

- 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

Lab:

- 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, Packet Captures (PCAPs), and Alerts of an Attack

- Investigate Browser-Based Attacks
- Analyze Suspicious Domain Name System (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

Intended Audience

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

Prerequisites

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

Follow-on Courses

Python for Network Automation

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.