Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

What you'll learn in this course

TThe Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) training provides an understanding of the network infrastructure devices, operations, and vulnerabilities of the TCP/IP protocol suite, and basic information security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data that are used to investigate security incidents. After completing this training, you will have the basic knowledge that is required to perform the job role of an associate-level cybersecurity analyst in a threat-centric security operations center (SOC).

This training prepares you for the 200-201 CBROPS v1.2 exam. If passed, you earn the Cisco Certified Cybersecurity 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 toward recertification

Course duration

- Instructor-led training: 5 days in the classroom with hands-on practice, plus the equivalent of 3 days of self-study material
- Virtual instructor-led training: 5 days of virtual instructor-led classes with hands-on practice, plus the equivalent of 3 days of self-study material
- E-learning: Equivalent of 5 days of content with videos, practice, and challenge plus 3 days of self-study material

How you'll benefit

This course 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

Who should enroll

This training is designed for associate-level cybersecurity analysts who are working in security operation centers.

Technology areas

- CyberOps

Course details

Objectives

After taking this course, you should be able to:

- Explain how a SOC operates and describe the different types of services that are performed from a Tier 1 SOC analyst's perspective
- 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 the Windows operating system features and functionality
- Provide an overview of the Linux operating system
- Understand common endpoint security technologies
- Explain the network security monitoring (NSM) tools that are available to the network security analyst
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts
- Explain the data that is available to the network security analyst
- Describe the basic concepts and uses of cryptography
- Understand the foundational cloud security practices, including deployment and service models, shared responsibilities, compliance frameworks, and identity and access management, to effectively secure cloud environments against cyberthreats
- Understand and implement advanced network security, data protection, secure application deployment, continuous monitoring, and effective disaster recovery strategies to secure cloud deployments
- Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors
- Identify the common attack vectors
- Identify malicious activities
- Identify patterns of suspicious behaviors
- Identify resources for hunting cyber threats
- Explain the need for event data normalization and event correlation
- Conduct security incident investigations
- Explain the use of a typical playbook in the SOC
- Describe a typical incident response plan and the functions of a typical computer security incident response team (CSIRT)

Course Prerequisites

Before taking this course, you should have the following knowledge and skills:

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

The following Cisco course can help you gain the knowledge you need to prepare for this course:

- Implementing and Administering Cisco Solutions (CCNA®)

What to Expect in the Exam

BUnderstanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS) v1.2 is a 120-minute exam associated with the Cisco Certified Cybersecurity Associate certification.
This exam tests your knowledge and skills related to:

- Security concepts
- Security monitoring
- Host-based analysis
- Network intrusion analysis
- Security policies and procedure

Outline

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

How to enroll

To enroll in the CBROPS course or explore our larger catalog of courses on Cisco Digital Learning, contact us at <training@fastlane-mea.com>

Lab outline

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