
6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: <http://www.ctclc.com>

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

The **Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.2** 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).

How You'll Benefit

This training 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; 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.
- Earn 30 CE credits toward recertification

What to Expect in the Exam

Understanding 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 procedures

Objective

Upon completing this course, the student will 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)

Price :
\$4295.00
Duration :
5 Days
Certification Exam:
200-201
CE Credit: 30

Who Should Attend

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

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

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

These skills can be found in the following Cisco Learning Offering:

- Implementing and Administering Cisco Solutions (CCNA)

Course Outline

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 Resources for Hunting Cyber Threats**
- Module 15: Understanding Event Correlation and Normalization**
- Module 16: Identifying Common Attack Vectors**
- Module 17: Identifying Malicious Activity**
- Module 18: Identifying Patterns of Suspicious Behavior**
- Module 19: Identifying Resources for Hunting Cyber Threats**
- Module 20: Understanding Event Correlation and Normalization**
- Module 21: Conducting Security Incident Investigations**
- Module 22: Using a Playbook Model to Organize Security Monitoring**
- Module 23: Describing Incident Response**

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