

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

ID CBROPS **Price** 3,950.— €(excl. tax) **Duration** 5 days

Course Overview

The **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. **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
- Earn 30 CE credits toward recertification

What to Expect in the Exam

The 200-201 CBROPS exam is a 120-minute assessment for the Cisco Certified CyberOps Associate certification and is aligned with the associate-level cybersecurity operations analyst job role. The CBROPS exam tests a candidate's knowledge and skills related to security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures.

Who should attend

This training is designed for individuals seeking a role as an associate-level cybersecurity analyst and IT professionals desiring knowledge in Cybersecurity operations or those in pursuit of the Cisco Certified CyberOps Associate certification including:

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

This course is part of the following Certifications

Cisco Certified Cybersecurity Associate / CCNA Cybersecurity (CCNA CYBERSECURITY)

Prerequisites

Before taking this training, 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 \(CCNA\) v2.2](#)

Course Objectives

After taking this training, 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)

- 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

Detailed Course 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

About Fast Lane



Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.



Worldwide Presence
with high-end training centers
around the globe



Multiple Awards
from vendors such as AWS,
Microsoft, Cisco, Google, NetApp,
VMware



Experienced SMEs
with over 19.000 combined
certifications

Germany
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Austria
ITLS GmbH
(Partner of Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Switzerland
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch