Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

ID CBROPS **Price** CHF 4,670.—(excl. VAT) **Duration** 5 days

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 (CCCA)

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:

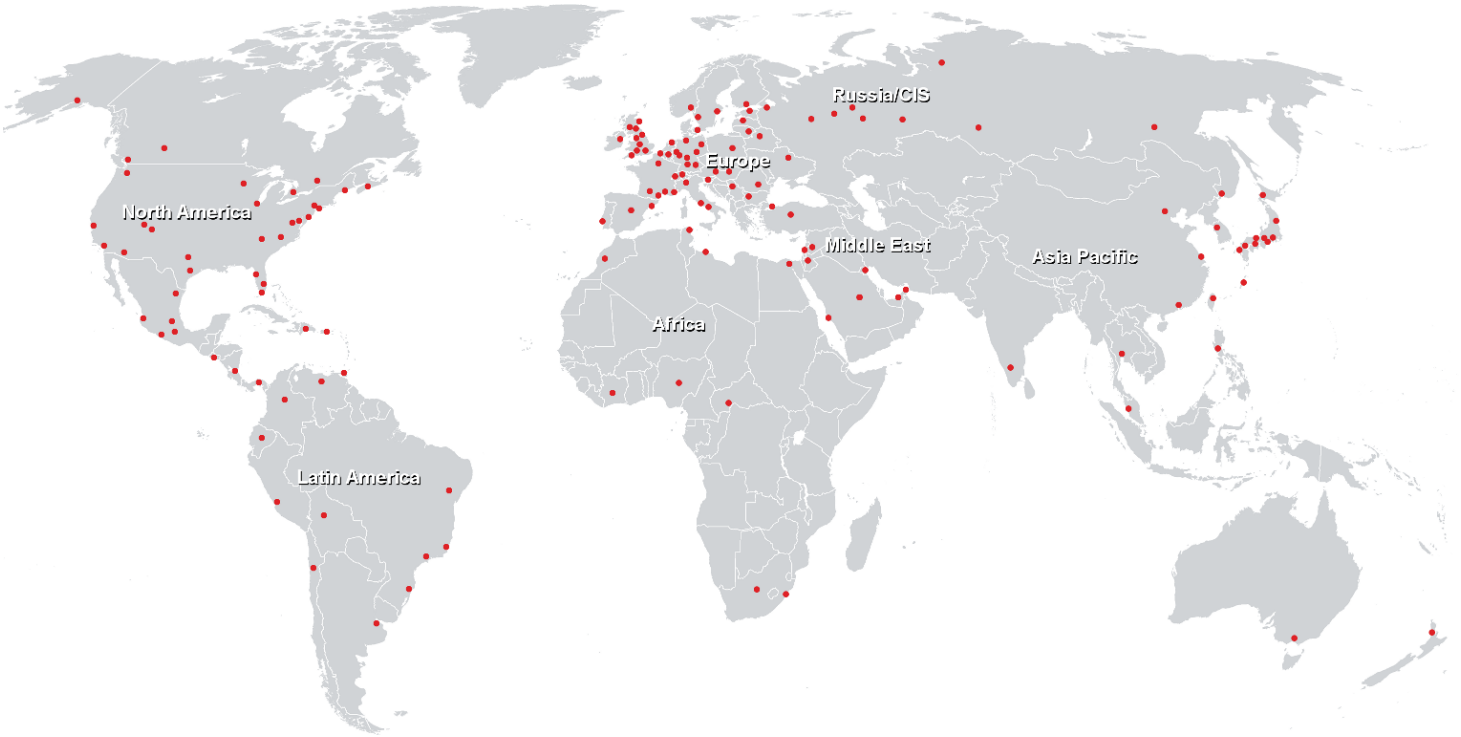
Implementing and Administering Cisco Solutions (CCNA)

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)

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch