Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

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

Who should attend

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

This course is part of the following Certifications

Cisco Certified CyberOps Associate (CCCA)

Prerequisites

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

- Skills and knowledge equivalent to those learned in Implementing and Administering Cisco Solutions (CCNA)
- 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

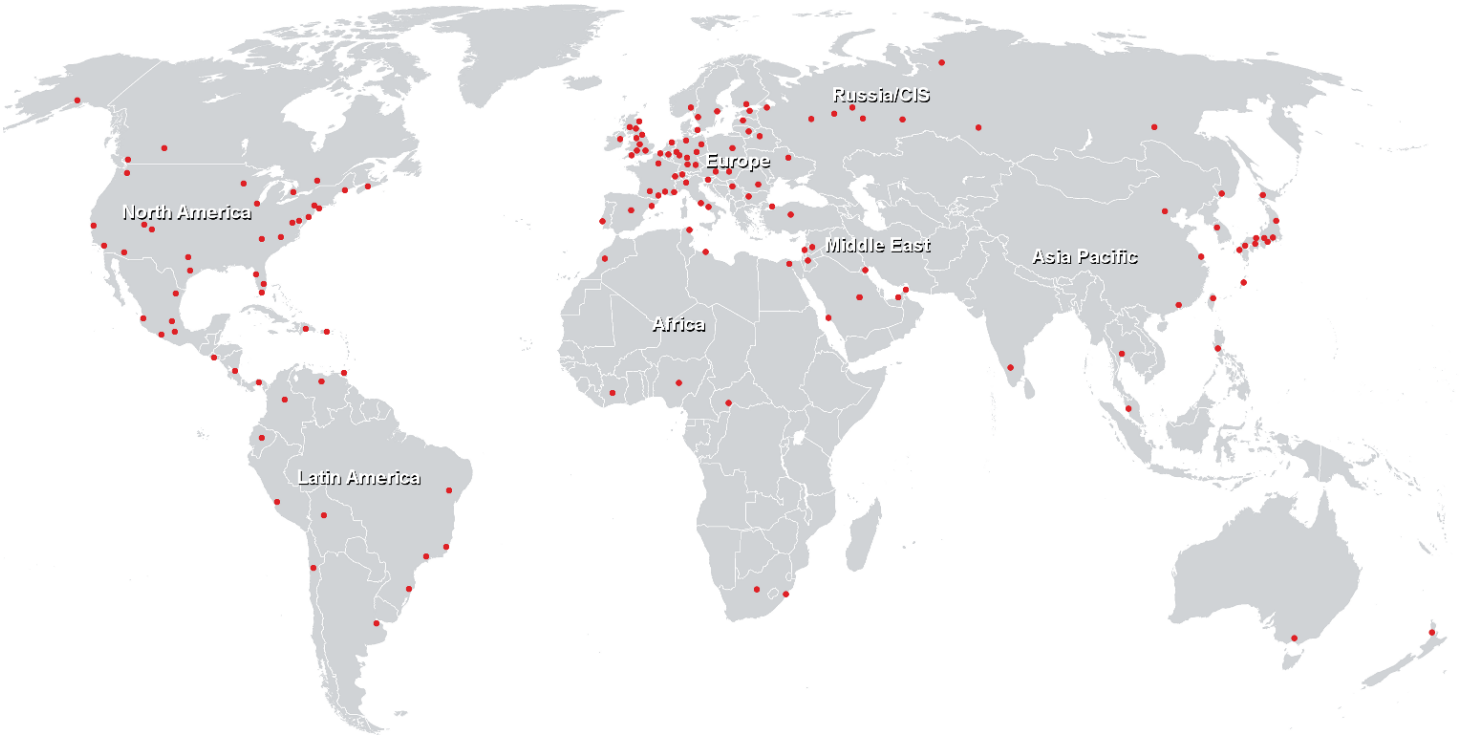
After taking this course, you should be able to:

- Explain how a SOC operates and describe the different types of services that are performed from a Tier 1 SOC analyst's perspective.
- Explain 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 CSIRT.
- Explain the use of VERIS to document security incidents in a standard format.
- Describe the Windows operating system features and functionality.
- Describe the Linux operating system features and functionality.

This course will help you:

- Gain the knowledge and skills to implement protocol that modernizes and tailors your network infrastructure.
- Learn hands-on training to streamline, design, and configure security measures to fortify your networks against Cybersecurity attacks.

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer GmbH

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

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