

# Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

ID CBROPS Preis CHF 4'670.– (exkl. MwSt.) Dauer 5 Tage

## Zielgruppe

Dieser Kurs richtet sich an Cybersecurity-Analysten auf Associate-Ebene, die in Sicherheitszentren arbeiten.

## Empfohlenes Training für die Zertifizierung zum

Cisco Certified Cybersecurity Associate (CCCA)

## Voraussetzungen

Vor der Teilnahme an diesem Kurs sollten Sie über die folgenden Kenntnisse und Fähigkeiten verfügen:

- Fertigkeiten und Kenntnisse, die denen entsprechen, die in [Implementing and Administering Cisco Solutions \(CCNA\)](#)
- Vertrautheit mit Ethernet und TCP/IP-Netzwerken
- Gute Kenntnisse der Betriebssysteme Windows und Linux
- Vertrautheit mit den Grundlagen von Netzwerksicherheitskonzepten

Der folgende Cisco-Kurs kann Ihnen helfen, das Wissen zu erwerben, das Sie zur Vorbereitung auf diesen Kurs benötigen:

[Implementing and Administering Cisco Solutions \(CCNA\)](#)

## Kursziele

Nach der Teilnahme an diesem Kurs sollten Sie in der Lage sein:

- Erläutern Sie die Funktionsweise eines SOC und beschreiben Sie die verschiedenen Arten von Dienstleistungen, die aus der Sicht eines Tier-1-SOC-Analysten erbracht werden.
- Erläuterung der Tools zur Überwachung der Netzwerksicherheit (Network Security Monitoring, NSM), die dem Netzwerksicherheitsanalysten zur Verfügung stehen.
- Erläutern Sie die Daten, die dem Netzwerksicherheitsanalysten zur Verfügung stehen.
- Beschreiben Sie die grundlegenden Konzepte und

Anwendungen der Kryptographie.

- Beschreiben Sie Sicherheitslücken im TCP/IP-Protokoll und wie diese für Angriffe auf Netzwerke und Hosts genutzt werden können.
- Verstehen gängiger Sicherheitstechnologien für Endgeräte.
- Verstehen der Kill Chain und der Diamantenmodelle für die Untersuchung von Vorfällen sowie der Verwendung von Exploit-Kits durch Bedrohungsakteure.
- Ermittlung von Ressourcen für die Jagd auf Cyber-Bedrohungen.
- Erklären Sie die Notwendigkeit der Normalisierung von Ereignisdaten und der Ereigniskorrelation.
- Identifizieren Sie die gängigen Angriffsvektoren.
- Identifizieren Sie bösartige Aktivitäten.
- Erkennen Sie verdächtige Verhaltensmuster.
- Durchführung von Untersuchungen von Sicherheitsvorfällen.
- Erklären Sie die Verwendung eines typischen Playbooks im SOC.
- Erläuterung der Verwendung von SOC-Metriken zur Messung der Wirksamkeit des SOC.
- Erläutern Sie den Einsatz eines Workflow-Management-Systems und der Automatisierung zur Verbesserung der Effizienz des SOC.
- Beschreiben Sie einen typischen Reaktionsplan auf Zwischenfälle und die Funktionen eines typischen CSIRT.
- Erläuterung der Verwendung von VERIS zur Dokumentation von Sicherheitsvorfällen in einem Standardformat.
- Beschreiben Sie die Merkmale und Funktionen des Windows-Betriebssystems.
- Beschreiben Sie die Merkmale und Funktionen des Betriebssystems Linux.

Dieser Kurs wird Ihnen helfen:

- Erwerben Sie das Wissen und die Fähigkeiten zur Implementierung von Protokollen, die Ihre Netzwerkinfrastruktur modernisieren und anpassen.
- Lernen Sie in praktischen Übungen, wie Sie Sicherheitsmassnahmen optimieren, entwerfen und konfigurieren, um Ihre Netzwerke gegen Cybersecurity-Angriffe zu schützen.

## Weltweite Trainingscenter



## 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>