Performing CyberOps Using Cisco Security Technologies (CBRCOR)

ID CBRCOR **Preis** CHF 4'200.– (exkl. MwSt.) **Dauer** 5 Tage

Zielgruppe

Obwohl es keine zwingenden Voraussetzungen gibt, ist der Kurs besonders für die folgenden Zielgruppen geeignet:

- Cybersecurity-Ingenieur
- Cybersecurity-Ermittler
- Vorfallsmanager
- Ansprechpartner für Vorfälle
- Netzwerktechniker
- SOC-Analysten, die derzeit auf Einstiegsebene tätig sind und über mindestens 1 Jahr Erfahrung verfügen

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Cybersecurity Professional (CCCP)

Voraussetzungen

Obwohl es keine zwingenden Voraussetzungen gibt, sollten Sie über die folgenden Kenntnisse verfügen, um von diesem Kurs profitieren zu können:

- Vertrautheit mit UNIX/Linux-Shells (bash, csh) und Shell-Befehlen
- Vertrautheit mit den Such- und Navigationsfunktionen von Splunk
- Grundlegende Kenntnisse der Skripterstellung unter Verwendung von Python, JavaScript, PHP o.ä.

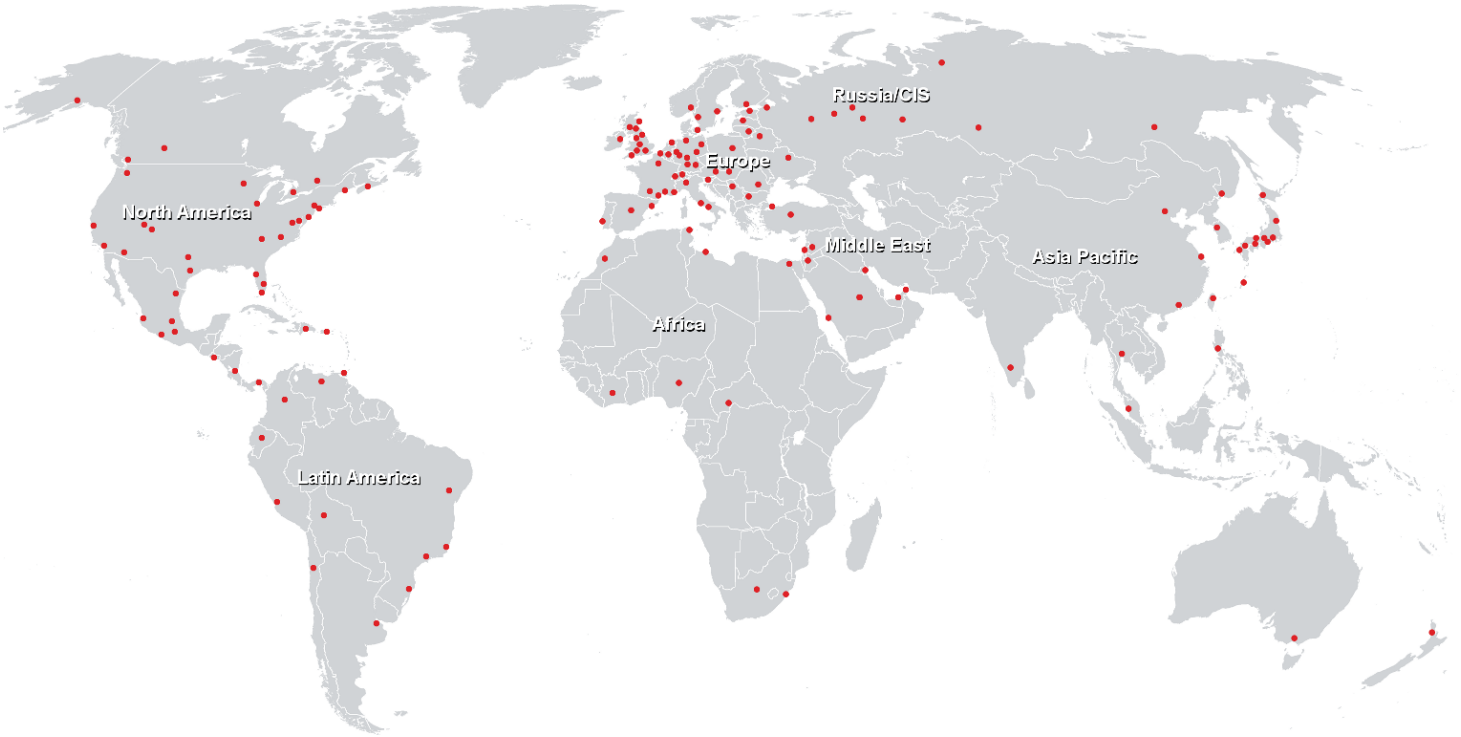
Empfohlene Cisco-Angebote, die Ihnen bei der Vorbereitung auf diesen Kurs helfen können:

- Implementing and Administering Cisco Solutions (CCNA)
- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Kursziele

- Beschreiben Sie die Arten der Dienstabdeckung innerhalb einer SOC und die damit verbundenen operativen Verantwortlichkeiten
- Vergleich der Sicherheitsaspekte von Cloud-Plattformen
- Beschreiben Sie die allgemeinen Methoden der Entwicklung, Verwaltung und Automatisierung von SOC-Plattformen
- Beschreibung der Segmentierung von Vermögenswerten, der Segregation, der Netzwerksegmentierung, der Mikrosegmentierung und der jeweiligen Ansätze als Teil der Kontrolle und des Schutzes von Vermögenswerten
- Beschreiben Sie Zero Trust und damit verbundene Ansätze als Teil der Vermögenskontrolle und des Vermögensschutzes
- Durchführung von Vorfallsuntersuchungen unter Verwendung von Security Information and Event Management (SIEM) und/oder Security Orchestration and Automation (SOAR) im SOC
- Verwendung verschiedener Arten von zentralen Sicherheitstechnologieplattformen für die Sicherheitsüberwachung, Untersuchung und Reaktion
- Beschreiben Sie die DevOps- und SecDevOps-Prozesse
- Beschreiben Sie die gängigen Datenformate (z. B. JavaScript Object Notation (JSON), HTML, XML und Comma-Separated Values (CSV)).
- Beschreiben Sie API-Authentifizierungsmechanismen
- Analyse des Ansatzes und der Strategien zur Erkennung von Bedrohungen während der Überwachung, Untersuchung und Reaktion
- Ermitteln bekannter Indikatoren für die Gefährdung (IOCs) und Indikatoren für Angriffe (IOAs)
- Interpretation der Abfolge von Ereignissen während eines Angriffs auf der Grundlage einer Analyse der Verkehrsmuster
- Beschreiben Sie die verschiedenen Sicherheitstools und ihre Grenzen für die Netzwerkanalyse (z. B. Tools zur Paketaufzeichnung, zur Analyse des Datenverkehrs und zur Analyse von Netzwerkprotokollen)
- Analysieren Sie anomales Nutzer- und Entitätsverhalten (UEBA)
- Proaktive Bedrohungssuche nach bewährten Verfahren

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