Implementing and Operating Cisco Security Core Technologies (SCOR)

ID SCOR **Preis** CHF 4'150.– (exkl. MwSt.) **Dauer** 5 Tage

Zielgruppe

- Sicherheitsingenieur
- Netzwerktechniker
- Netzwerk-Designer
- Netzwerkadministrator
- Systemingenieur
- Beratender Systemingenieur
- Architekt für technische Lösungen
- Cisco Integratoren/Partner
- Netzwerk-Manager
- Cisco Integratoren und Partner

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Network Professional Security (CCNP SECURITY)

Voraussetzungen

Um von diesem Kurs in vollem Umfang zu profitieren, sollten Sie über die folgenden Kenntnisse und Fähigkeiten verfügen:

- Fertigkeiten und Kenntnisse, die denen des Kurses Implementing and Administering Cisco Solutions (CCNA) v1.0 entsprechen
- Vertrautheit mit Ethernet und TCP/IP-Netzwerken
- Kenntnisse im Umgang mit dem Betriebssystem Windows
- Kenntnisse über Cisco IOS-Netzwerke und Konzepte
- Vertrautheit mit den Grundlagen von Netzwerksicherheitskonzepten

Kursziele

Nach dem Besuch dieses Kurses sollten Sie in der Lage sein:

- Konzepte und Strategien der Informationssicherheit im Netzwerk beschreiben
- Beschreiben Sie gängige TCP/IP-, Netzwerkanwendungs- und Endpunkt-Angriffe
- Beschreiben, wie verschiedene Netzwerksicherheitstechnologien zum Schutz vor Angriffen zusammenarbeiten
- Zugriffskontrolle auf Cisco ASA-Appliance und Cisco Firepower Next-Generation Firewall implementieren
- Beschreiben und Implementieren grundlegender Sicherheitsmerkmale und -funktionen für E-Mail-Inhalte, die von der Cisco Email Security Appliance bereitgestellt werden
- Beschreiben und Implementieren der von der Cisco Web Security Appliance bereitgestellten Features und Funktionen für die Sicherheit von Webinhalten
- Beschreiben Sie die Sicherheitsfunktionen von Cisco Umbrella, die Bereitstellungsmodelle, die Richtlinienverwaltung und die Untersuchungskonsole
- VPNs einführen und Kryptographie-Lösungen und -Algorithmen beschreiben
- Beschreiben Sie Cisco-Lösungen für sichere Site-to-Site-Konnektivität und erklären Sie, wie Sie Cisco IOS VTI-basierte Punkt-zu-Punkt-IPsec-VPNs und Punkt-zu-Punkt-IPsec-VPNs auf der Cisco ASA und der Cisco FirePower NGFW implementieren
- Beschreiben und Bereitstellen von Cisco Secure Remote Access Connectivity-Lösungen und Beschreiben der Konfiguration von 802.1X und EAP-Authentifizierung
- Vermittlung eines grundlegenden Verständnisses der Endpunktsicherheit und Beschreibung der Architektur und der grundlegenden Funktionen von AMP for Endpoints
- Untersuchen Sie verschiedene Verteidigungsmassnahmen auf Cisco-Geräten, die die Kontroll- und Verwaltungsebene schützen
- Konfigurieren und verifizieren Sie die Cisco IOS Software Layer 2 und Layer 3 Data Plane Controls
- Beschreiben Sie die Lösungen Cisco Stealthwatch Enterprise und Stealthwatch Cloud
- Beschreiben Sie die Grundlagen des Cloud Computing und gängige Cloud-Angriffe und wie man eine Cloud-Umgebung absichert.

Dieser Kurs wird Ihnen helfen:

- Sammeln Sie praktische Erfahrungen bei der Implementierung zentraler Sicherheitstechnologien und lernen Sie Best Practices mit Cisco Sicherheitslösungen kennen
- Bereiten Sie sich auf die Prüfung Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) vor

- Qualifizieren Sie sich für Sicherheitsjobs auf Fach- und Expertenebene

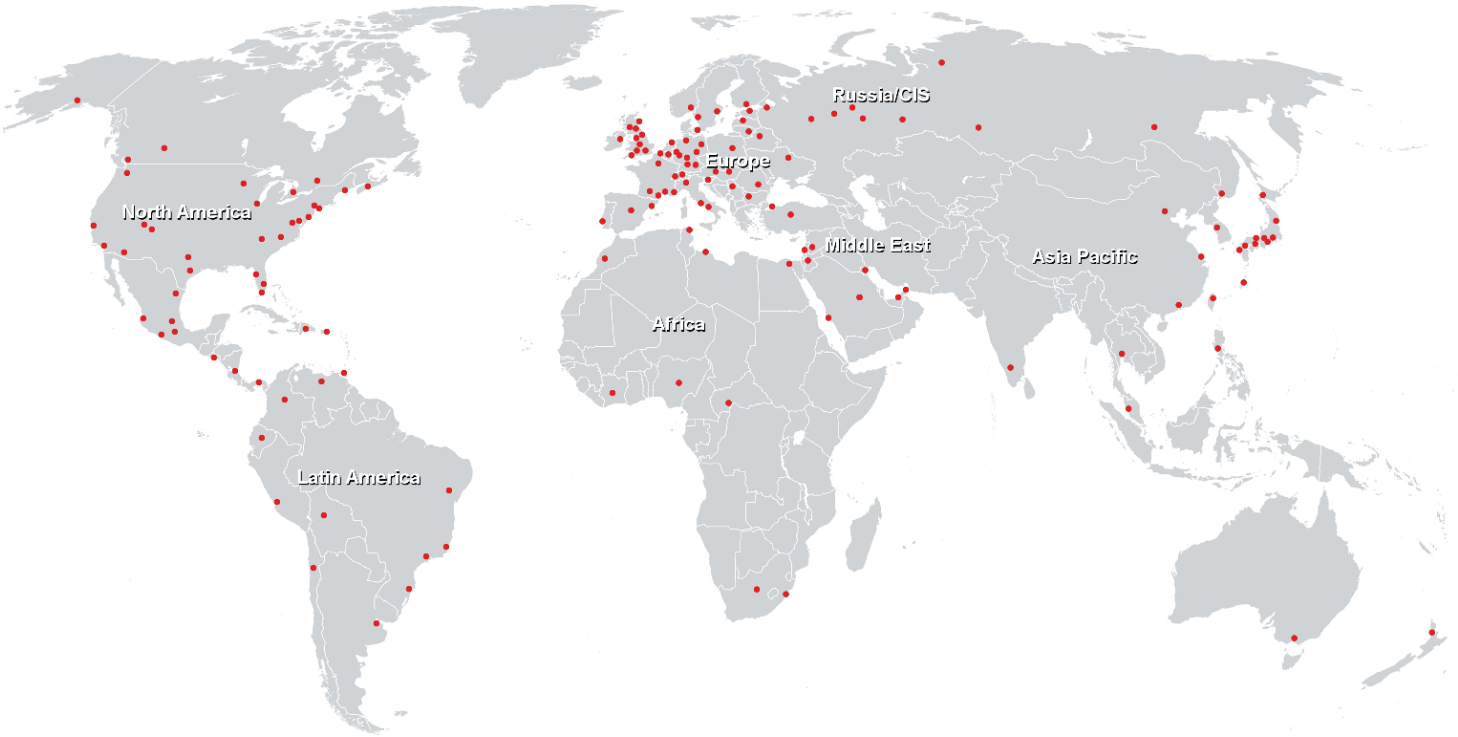
Dieser Kurs unterstützt Sie bei der Vorbereitung auf die Prüfung Implementing and Operating Cisco Security Core Technologies (350-701 SCOR). Diese Prüfung testet das Wissen eines Kandidaten über die Implementierung und den Betrieb von Kernsicherheitstechnologien.

Kursinhalt

- Beschreiben von Informationssicherheitskonzepten*
- Beschreibung gängiger TCP/IP-Angriffe*
- Beschreibung gängiger Angriffe auf Netzwerkanwendungen*
- Beschreibung gängiger Endpunkt-Angriffe*
- Beschreiben von Netzwerksicherheitstechnologien
- Einsatz der Cisco ASA Firewall
- Einsatz der Cisco Firepower Next-Generation Firewall
- Einsatz von E-Mail-Inhaltssicherheit
- Einsatz von Web Content Security
- Einsatz von Cisco Umbrella*
- Erklärungen zu VPN-Technologien und Kryptographie
- Einführung in die sicheren Site-to-Site-VPN-Lösungen von Cisco
- Einsatz von Cisco IOS VTI-basiertem Punkt-zu-Punkt
- Bereitstellen von Punkt-zu-Punkt-IPsec-VPNs auf der Cisco ASA und Cisco Firepower NGFW
- Einführung in die Cisco Secure Remote Access VPN-Lösungen
- Bereitstellen von Remote Access SSL-VPNs auf der Cisco ASA und Cisco Firepower NGFW
- Erklärungen zu Cisco Secure Network Access-Lösungen
- Beschreiben der 802.1X-Authentifizierung
- Konfigurieren der 802.1X-Authentifizierung
- Beschreibung der Endpunktsicherheitstechnologien*
- Bereitstellen von Cisco AMP für Endpunkte*
- Einführung in den Schutz der Netzwerkinfrastruktur*
- Einsatz von Sicherheitskontrollen der Steuerungsebene*
- Einsatz von Layer 2 Data Plane Security Controls*
- Einsatz von Layer 3 Data Plane Security Controls*
- Einsatz von Sicherheitskontrollen der Managementebene*
- Einsatz von Verkehrstelemetrie-Methoden*
- Einsatz von Cisco Stealthwatch Enterprise*
- Beschreibung der Cloud und gängiger Cloud-Angriffe*
- Absicherung der Cloud*
- Bereitstellen von Cisco Stealthwatch Cloud*
- Beschreiben von Software-Defined Networking (SDN*)

Dieser Abschnitt ist Material zum Selbststudium, das Sie in Ihrem eigenen Tempo bearbeiten können, wenn Sie die von einem Kursleiter geleitete Version dieses Kurses besuchen.

Weltweite Trainingscenter



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