Implementing Security Service Edge with Cisco Secure Access (ICSA)

ID ICSA **Preis** auf Anfrage **Dauer** 3 Tage

Zielgruppe

- Sicherheitsingenieure
- Sicherheitsadministratoren
- Netzwerksicherheitsingenieure
- Cloud-Sicherheitsingenieure
- Sicherheitsarchitekten
- Sicherheitsberater
- Systemingenieure
- Infrastrukturingenieure
- SOC-Analysten
- Spezialisten für Zero-Trust-Sicherheit

Voraussetzungen

Für diese Schulung gibt es keine formalen Voraussetzungen. Es wird jedoch empfohlen, dass Sie vor der Teilnahme an dieser Schulung über folgende Kenntnisse und Fähigkeiten verfügen:

- Mindestens 2 Jahre Berufserfahrung im Bereich Netzwerksicherheit oder Sicherheitsadministration
- Grundlegendes Verständnis von Routing und Switching in Unternehmensnetzwerken
- Grundlegendes Verständnis der Konzepte im Bereich WAN-Netzwerke
- Grundlegendes Verständnis von VPN-Technologien (IPsec, SSL/TLS)
- Grundlegendes Verständnis von DNS, HTTP/HTTPS und Konzepten der Websicherheit
- Grundlegendes Verständnis der Zero-Trust-Prinzipien
- Kenntnisse über Cloud-basierte Sicherheitsdienste

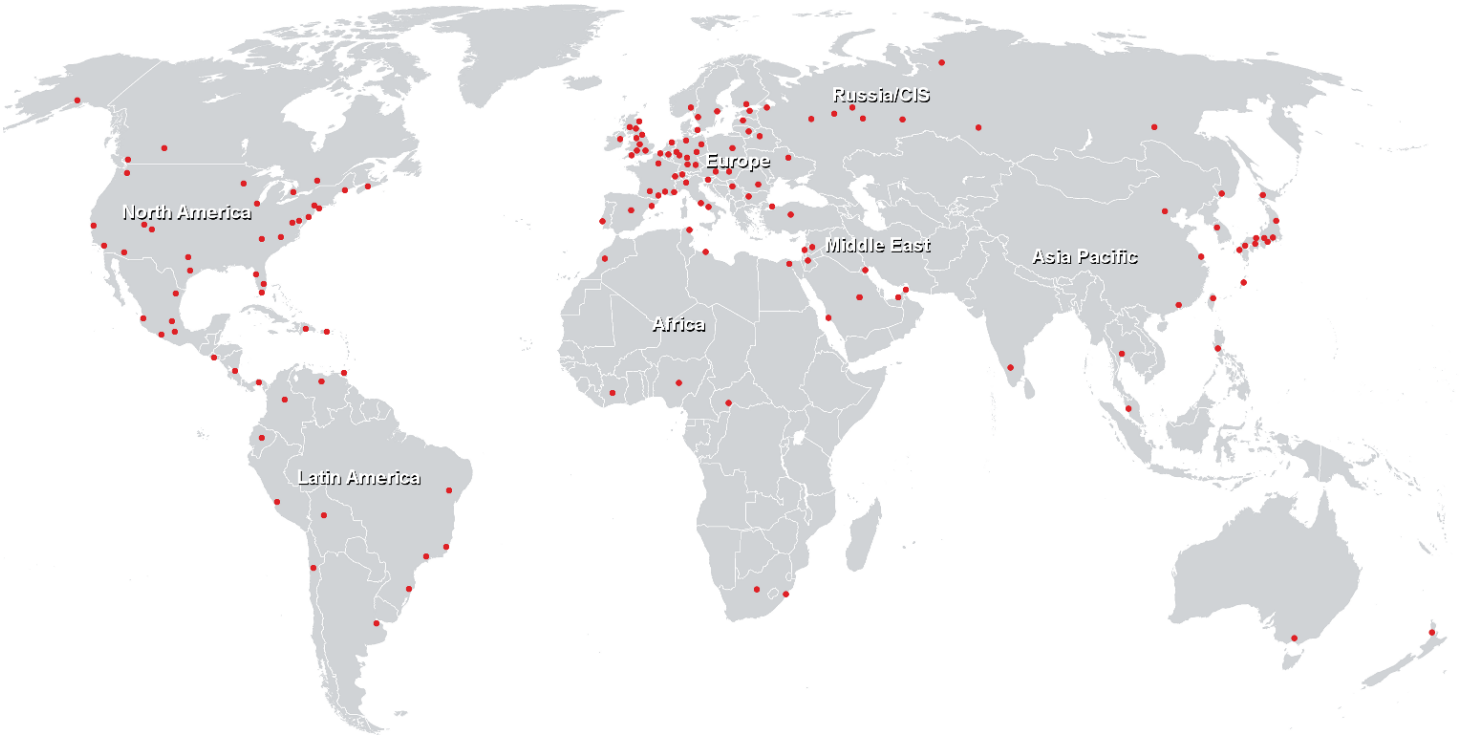
Diese Kenntnisse werden in den folgenden Cisco-Schulungsangeboten vermittelt:

- Implementing and Operating Cisco Security Core Technologies (SCOR)
- Implementing and Administering Cisco Solutions (CCNA)
- Cisco SDWAN Fundamentals (SDWFND)
- Implementing Cisco SD-WAN Solutions (ENSDWI)

Kursziele

- Beschreiben Sie die SASE-Frameworks, die darin enthaltenen cloudbasierten SSE-Sicherheitsdienste sowie die SD-WAN-Konzepte und die integrierten Sicherheitsfunktionen der Cisco SD-WAN-Edge-Geräte, die die SASE-Architektur vervollständigen.
- Beschreiben Sie die Architektur der Cisco Secure Access-Plattform und die wichtigsten Anwendungsfälle.
- Beschreiben Sie die Verwaltungsoptionen von Cisco Secure Access und das Admin-Portal
- Beschreiben Sie die Bausteine des Workflows für die Erstkonfiguration von Cisco Secure Access.
- Beschreiben Sie die in Cisco Secure Access verfügbaren Methoden zur Erfassung des Datenverkehrs auf der Benutzerseite und die Backhaul-Methoden für private Anwendungen.
- Konfigurieren der Benutzerverwaltung für Cisco Secure Access und der SAML-basierten SSO-Authentifizierung
- Konfigurieren Sie die für „Secure Private Access“ erforderlichen allgemeinen Cisco Secure Access-Komponenten, darunter die anwendungsseitige Konnektivität, die Definition privater Ressourcen und die Zugriffsrichtlinien.
- Konfigurieren Sie den Zero-Trust-Zugriff in Cisco Secure Access mithilfe clientbasierter und browserbasierter Methoden
- Konfigurieren von VPNaaS und Branch IPsec in Cisco Secure Access für sicheren privaten Zugriff
- Konfigurieren von Endpunkt-Sicherheitsstatus-, Sicherheits- und IPS-Profilen in Cisco Secure Access für Secure Private Access
- Konfigurieren Sie die allgemeinen Cisco Secure Access-Komponenten, die für den sicheren Internetzugang erforderlich sind
- Beschreiben Sie die Zugriffsmethoden für den sicheren Internetzugang in Cisco Secure Access.
- Konfigurieren Sie die Funktionen zum Schutz vor Bedrohungen und zur Inhaltsfilterung in Cisco Secure Access for Secure Internet Access
- Konfigurieren von Data Loss Prevention in Cisco Secure Access
- Überprüfen Sie die Benutzererfahrung von Cisco Secure Access mithilfe von Experience Insights
- Integrieren Sie Cisco Secure Access mit Cisco XDR und Splunk Enterprise, um den SOC-Betrieb zu optimieren

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