Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)

ID SCAZT **Preis** auf Anfrage **Dauer** 5 Tage

Zielgruppe

- Netzwerk-Ingenieure
- Netzwerksicherheitsingenieure
- Netzwerk-Architekten
- Vertrieb/Verkaufsingenieure

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Network Professional Security (CCNP SECURITY)

Voraussetzungen

Die Kenntnisse und Fähigkeiten, die Sie vor der Teilnahme an dieser Schulung haben sollten, sind

- Grundlegendes Verständnis von Enterprise Routing
- Grundlegendes Verständnis von WAN-Netzwerken
- Grundlegendes Verständnis von Cisco SD-WAN
- Grundlegendes Verständnis von Public Cloud-Diensten

Diese Fähigkeiten können in den folgenden Cisco-Lernangeboten erworben werden:

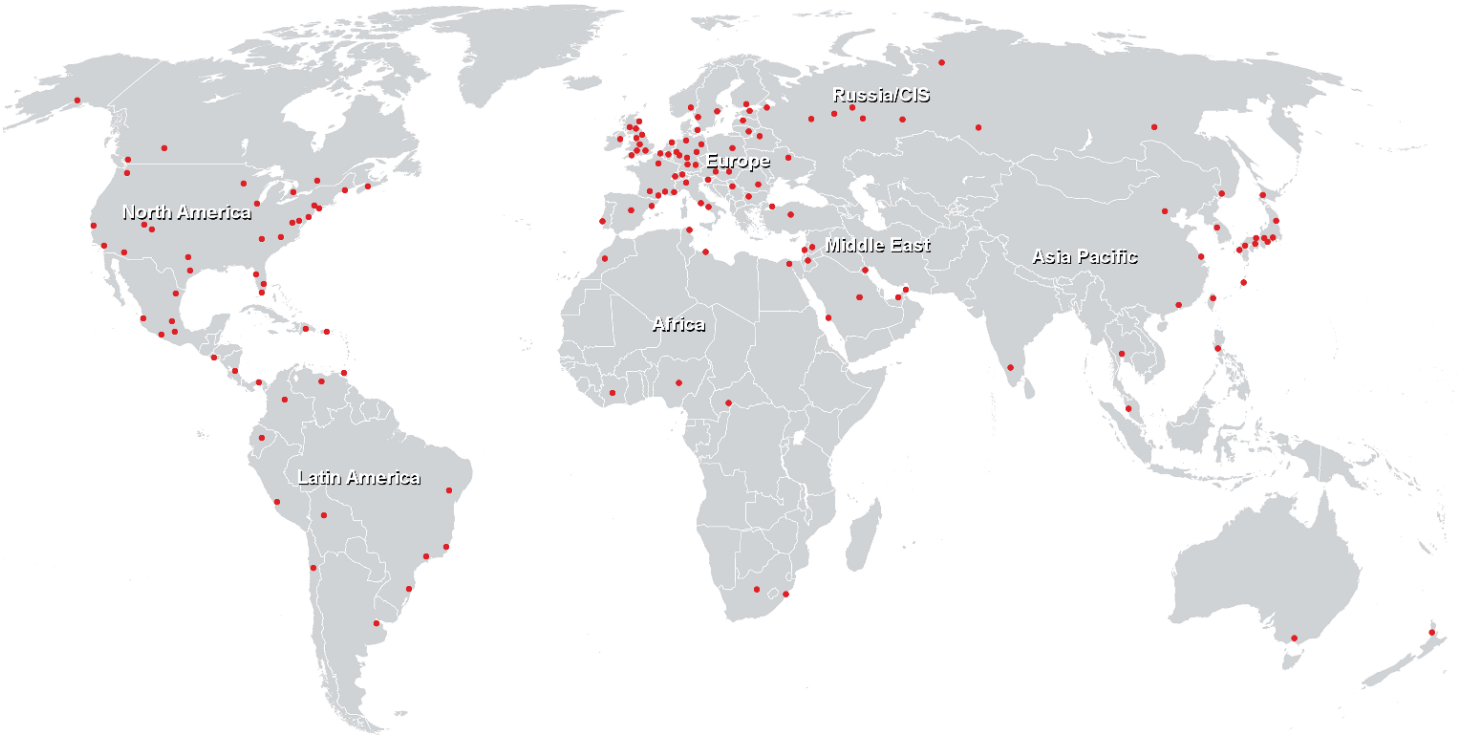
- Implementing and Administering Cisco Solutions (CCNA)
- !Implementing Cisco SD-WAN Solutions (ENSDWI)
- Cisco SD-WAN Operation and Deployment (SDWFND)

Kursziele

- Vergleich und Gegenüberstellung der Sicherheitsrahmenwerke des National Institute of Standards and Technology (NIST), der Cybersecurity and Infrastructure Security Agency (CISA) und der Defense Information Systems Agency (DISA) sowie Verständnis für die Bedeutung der Übernahme standardisierter Rahmenwerke für die Cybersicherheit zur Verbesserung der Sicherheitslage eines Unternehmens
- Beschreiben Sie die Cisco Security Reference Architecture und ihre fünf Hauptkomponenten
- Beschreibung gängiger Anwendungsfälle und Empfehlung der erforderlichen Fähigkeiten innerhalb einer integrierten Sicherheitsarchitektur, um diese effektiv zu bewältigen
- Beschreiben Sie die Cisco Secure Architecture for Everyone (SAFE) Architektur
- Überprüfung der Vorteile, Komponenten und Verfahren der zertifikatsbasierten Authentifizierung für Benutzer und Geräte
- Aktivieren Sie die Duo-Multifaktor-Authentifizierung (MFA), um eine Anwendung vom Duo-Administrationsportal aus zu schützen, und konfigurieren Sie dann die Anwendung so, dass sie Duo MFA für die Authentifizierung der Benutzeranmeldung verwendet
- Installieren Sie Cisco Duo und implementieren Sie die Multifaktor-Authentifizierung im virtuellen privaten Netzwerk (VPN) für den Fernzugriff.
- Konfigurieren der Endpunktkonformität
- Überprüfung und Nachweis der Fähigkeit, Stateful Switchover (SSO) unter Verwendung der Security Assertion Markup Language (SAML) oder OpenID Connect in Verbindung mit Cisco Duo zu verstehen
- Beschreiben Sie die Cisco Software-defined Wide-Area Network (SD-WAN) On-Box- und integrierten Threat Prevention Security Services
- Beschreiben Sie die SD-WAN On-Box- und integrierten Content-Filtering-Sicherheitsdienste
- Beschreiben Sie die Funktionen und Möglichkeiten von Cisco Umbrella Secure Internet Gateway (SIG), wie DNS-Sicherheit, Cloud-Delivered Firewall (CDFW), Intrusion Prevention Systems (IPS) und Interaktion mit Cisco SD-WAN
- Einführung des Reverse-Proxys für den Schutz von Anwendungen mit Internetzugang
- Erkunden Sie den Anwendungsfall von Cisco Umbrella SIG zur Sicherung des Zugriffs auf Cloud-Anwendungen, die Einschränkungen und Vorteile der Lösung sowie die verfügbaren Funktionen zur Erkennung und Kontrolle des Zugriffs auf Cloud-Anwendungen
- Entdecken Sie die Cisco ThousandEyes-Funktionen zur Überwachung der Cisco SD-WAN-Bereitstellung
- Beschreiben Sie die Herausforderungen beim Zugriff auf SaaS-Anwendungen in modernen Geschäftsumgebungen und lernen Sie die Cisco SD-WAN Cloud OnRamp for SaaS-Lösung mit direktem oder zentralisiertem Internetzugang kennen
- Einführung in die Cisco Secure Firewall-Plattformen, Anwendungsfälle und Sicherheitsfunktionen

- ein umfassendes Verständnis von Web Application Firewalls nachweisen
- Demonstration eines umfassenden Verständnisses der Funktionen, Bereitstellungsoptionen, Agenten und Konnektoren von Cisco Secure Workload
- Demonstration eines umfassenden Verständnisses von Cisco Secure Workload Application Dependency Mapping und Policy Discovery
- Demonstration eines umfassenden Verständnisses gängiger Cloud-Angriffstaktiken und Abhilfestrategien
- Demonstration eines umfassenden Verständnisses der Multi-Cloud-Sicherheitsanforderungen und -richtlinienfunktionen
- Einführung in die Sicherheitsprobleme bei der Einführung von öffentlichen Clouds und in die gemeinsamen Fähigkeiten von Cloud-Tools zur Sichtbarkeit und Sicherheit, um diese Probleme zu entschärfen
- Einführung in Cisco Secure Network Analytics und Cisco Security Analytics and Logging
- Beschreiben Sie das Cisco Attack Surface Management
- Beschreiben Sie, wie Anwendungsprogrammschnittstellen (APIs) und Automatisierung bei der Fehlersuche in der Cloud-Richtlinie helfen können, insbesondere im Zusammenhang mit Fehlkonfigurationen
- Demonstration umfassender Kenntnisse über die angemessenen Reaktionen auf Cloud-Bedrohungen in spezifischen Szenarien
- Demonstration der umfassenden Kenntnisse, die erforderlich sind, um die Automatisierung für die Erkennung von und Reaktion auf Cloud-Bedrohungen zu nutzen

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