# Designing Cisco Security Infrastructure (SDSI)

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

## Zielgruppe

- Systemingenieure von Cisco und Partnern
- Kunden-Netzwerk- und Infrastruktur-Ingenieure
- Kunden-Sicherheit/NOC-Ingenieure

## Empfohlenes Training für die Zertifizierung zum

Cisco Certified Network Professional Security (CCNP SECURITY)

## Voraussetzungen

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

- Cisco CCNP Security oder gleichwertige Kenntnisse
- Vertrautheit mit Microsoft Windows-Betriebssystemen
- Vertrautheit mit dem Cisco Security Portfolio

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

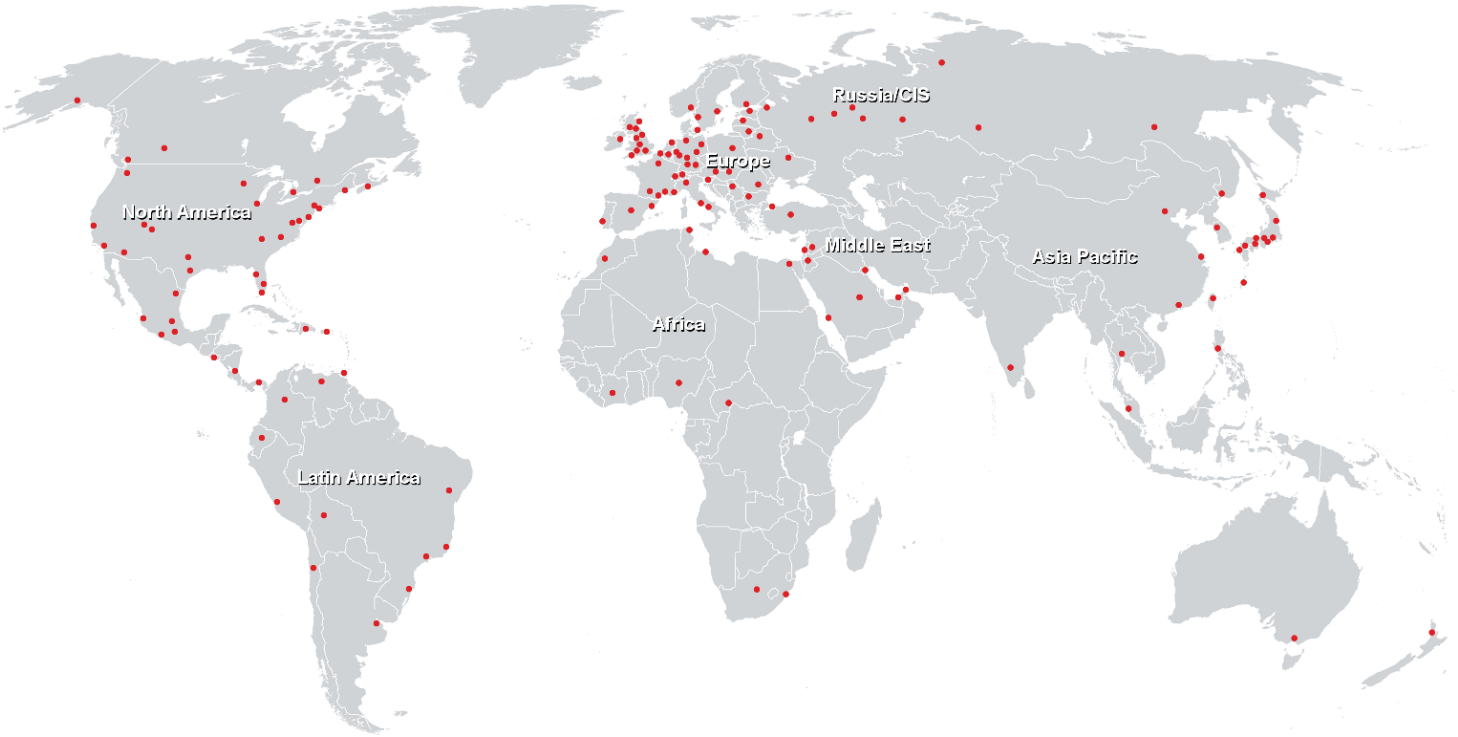
- Implementing and Operating Cisco Security Core Technologies (SCOR)
- Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF)
- Implementing and Configuring Cisco Identity Services Engine (SISE)
- Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)
- Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPA)
- Implementing Secure Solutions with Virtual Private Networks (SVPN)
- Introducing Automation for Cisco Solutions (CSAU)
- Securing Your Email with Cisco IronPort C-Series (SESA)
- Securing the Web with Cisco Web Security Appliance (SWSA)

## Kursziele

- Identifizierung und Erläuterung der grundlegenden Konzepte der Sicherheitsarchitektur und wie sie den Entwurf, den Aufbau und die Wartung einer sicheren Infrastruktur unterstützen
- Identifizierung der Schichten der Sicherheitsinfrastruktur, der wichtigsten Sicherheitstechnologien und der Infrastrukturkonzepte
- Erläutern, wie die Grundsätze des Sicherheitsdesigns zu einer sicheren Infrastruktur beitragen
- Identifizierung und Erörterung von Rahmenwerken für die Sicherheitsgestaltung und -verwaltung, die für die Gestaltung der Infrastruktursicherheit verwendet werden können
- Erläuterung der Bedeutung und der Methoden zur Durchsetzung der Einhaltung von Vorschriften bei der Sicherheitsgestaltung
- Identifizierung von Tools, die die Erkennung von und Reaktion auf Sicherheitsvorfälle in der Infrastruktur ermöglichen
- Erläuterung verschiedener Strategien, die zur Anpassung traditioneller Sicherheitsarchitekturen an die technischen Anforderungen moderner Unternehmensnetze eingesetzt werden können
- Implementierung sicherer Netzwerkzugriffsmethoden, wie 802.1X, MAC Authentication Bypass (MAB) und webbasierte Authentifizierung
- Beschreibung von Sicherheitstechnologien, die auf WAN-Verbindungen (Wide Area Network) von Unternehmen angewendet werden können
- Vergleich von Methoden zur Sicherung des Netzwerkmanagements und des Datenverkehrs auf der Steuerungsebene
- Vergleich der Unterschiede zwischen herkömmlichen Firewalls und Next-Gen-Firewalls (NGFWs) und Identifizierung der erweiterten Funktionen, die NGFWs bieten
- Erklären, wie Web Application Firewalls (WAFs) Webanwendungen vor Bedrohungen schützen
- Beschreibung der wichtigsten Merkmale und bewährten Verfahren für den Einsatz von Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS) als Teil des Sicherheitsdesigns der Unternehmensinfrastruktur
- Erklären Sie, wie Endpunkte und Dienste in Cloud-nativen oder Microservice-Umgebungen mit Host-basierten oder verteilten Firewalls geschützt werden können.
- Erörterung von Sicherheitstechnologien für Anwendungsdaten und Daten, die sich im Transit befinden
- Identifizierung verschiedener Sicherheitslösungen für Cloud-

native Anwendungen, Microservices und Container
- Erläutern Sie, wie der technologische Fortschritt die Sicherheit der heutigen Infrastrukturen verbessern kann.
- Identifizierung von Tools, die die Erkennung von und Reaktion auf Sicherheitsvorfälle in der Infrastruktur ermöglichen
- Beschreibung von Rahmenwerken und Kontrollen für den Zugang zu und die Minderung von Sicherheitsrisiken für Infrastrukturen
- Erläutern, wie nach einem Sicherheitsvorfall Sicherheitsanpassungen vorgenommen werden können
- Identifizierung von DevSecOps-Integrationen, die das Sicherheitsmanagement und die Reaktion verbessern
- Erörterung der Frage, wie die Sicherheit automatisierter Dienste gewährleistet werden kann
- Erörterung der Frage, wie KI bei der Erkennung von und Reaktion auf Bedrohungen helfen kann

**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**