SDSI
Designing Cisco Security Infrastructure

The Designing Cisco Security Infrastructure (SDSI) training course provides you with knowledge about the design of security architectures, including secure infrastructures, applications, risks, events, requirements, artificial intelligence (AI), automation, and DevSecOps.

Course Contents
- Identify and explain the fundamental concepts of security architecture and how they support the design, building, and maintenance of a secure infrastructure
- Identify the layers of security infrastructure, core security technologies, and infrastructure concepts
- Explain how security designs principles contribute to secure infrastructure
- Identify and discuss security design and management frameworks that can be used for infrastructure security design
- Explain the importance of and methods for enforcement of regulatory compliance in security design
- Identify tools that enable detection and response to infrastructure security incidents
- Explain various strategies that can be implemented to modify traditional security architectures to meet the technical requirements of modern enterprise networks
- Implement secure network access methods, such as 802.1X, MAC Authentication Bypass (MAB), and web-based authentication
- Describe security technologies that can be applied to enterprise Wide Area Network (WAN) connections
- Compare methods to secure network management and control plane traffic
- Compare the differences between traditional firewalls and next-gen firewalls (NGFWs) and identify the advanced features that NGFWs provide
- Explain how web application firewalls (WAFs) secure web applications from threats
- Describe the key features and best practices for deploying intrusion detection system (IDS) and intrusion prevention system (IPS) as part of the enterprise infrastructure security design
- Explain how endpoints and services in cloud-native or microservice environments can be protected with host-based or distributed firewalls
- Discuss security technologies that address application data and data that is in transit
- Identify several security solutions for cloud-native applications, microservices, and containers
- Explain how technology advancements allow for improvements in today's infrastructure security
- Identify tools that enable detection and response to infrastructure security incidents
- Describe frameworks and controls to access and mitigate security risks for infrastructure
- Explain how to make security adjustments following a security incident
- Identify DevSecOps integrations that improve security management and response
- Discuss how to ensure that automated services are secure
- Discuss how AI can aid in threat detection and response

E-Book You will receive the original course documentation from Cisco in English language as a Cisco E-Book.

Target Group
- Cisco and Partner's Systems Engineers
- Customer Network & Infrastructure Engineers
- Customer Security/NOC Engineers

Prerequisites
There are no prerequisites for this training. However, it is recommended that you have the following knowledge and skills before participating in this training:

- Cisco CCNP Security or equivalent knowledge
- Familiarity with Microsoft Windows operating systems
- Familiarity with the Cisco Security portfolio

These skills can be found in the following Cisco learning offerings:

- 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 Automation for Cisco Security Solutions (SAUI)
- Implementing Secure Solutions with Virtual Private Networks (SVPN)
- Introducing Automation for Cisco Solutions (CSAU)
- Securing Email with Cisco Email Security Appliance (SESA)
- Securing the Web with Cisco Web Security Appliance (SWSA)

Course Target
- Gain practical experience in designing security architectures
- Qualify for professional and experienced security tasks

After passing the exam, you will receive the **Cisco Certified Specialist – Designing Cisco Security Infrastructure** specialization and meet the requirements of the Concentration Exam for **CCNP® Security** certification.

Status 11/27/2025

Training		Prices, excl. of V.A.T.
Classes in Germany	**5 Days**	**€ 3,595**
Online Training	**5 Days**	**€ 3,595**

Date/course venue		Course language German 🇩🇪	
09/03-13/03/26	Düsseldorf	21/09-25/09/26	Düsseldorf
09/03-13/03/26	Online	21/09-25/09/26	Online
22/06-26/06/26	Frankfurt	07/12-11/12/26	Frankfurt
22/06-26/06/26	Online	07/12-11/12/26	Online

SDSI

Security

ExperTeach

Our Training Offer for You:

Classroom Training
The live training experience in our training centers or on your premises on-site.

Online Training
Attend your course in online mode – without travel and accommodation expenses and effort.

Hybrid Training
Classroom & online in one course – choose how you wish to participate in your training event.
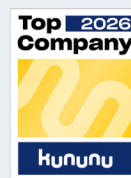
In-house Training
We create your customized training concepts for your project.

Guaranteed Course Dates
ExperTeach guaranteed course dates allow for secure and reliable planning.

Awards Won by ExperTeach