

## Designing Cisco Security Infrastructure

Durée: 5 Jours    Réf de cours: SDSI    Version: 1.0

### Résumé:

The **Designing Cisco Security Infrastructure (SDSI)** course teaches you about security architecture design, including secure infrastructure, applications, risk, events, requirements, artificial intelligence (AI), automation, and DevSecOps.

This training prepares you for the 300-745 SDSI exam. If passed, you earn the Cisco Certified Specialist – Designing Cisco Security Infrastructure certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Security certification.

**This Course is worth 41 Continuing Education (CE) credits toward recertification.**

### Public visé:

Individuals involved in the design of a Cisco security architecture

### Objectifs pédagogiques:

#### ■ After completing this course you should be able to:

- 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

---

## Pré-requis:

### Attendees should meet the following prerequisites:

- Cisco CCNP Security or Equivalent Knowledge
- Familiarity with Microsoft Windows Operating Systems
- Familiarity with the Cisco Security Portfolio
- CSAU - Présentation de l'automatisation pour les solutions Cisco
- SAUI - Implementing Automation for Cisco Security Solutions
- SCOR - Mettre en oeuvre et gérer les solutions de sécurité Cisco
- SISE - Mettre en oeuvre et configurer la solution Cisco Identity Services Engine
- SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention
- SFWIPA - Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention
- SWSA - Sécuriser le Web avec Cisco Web Security Appliance
- SVPN - Implementing Secure Solutions with Virtual Private Networks
- SCAZT - Designing and Implementing Secure Cloud Access for Users and Endpoints
- SESA - Sécuriser les emails avec Cisco Email Security Appliance

## Test et certification

### Recommended as preparation for the following exam:

- **300-745** - Designing Cisco Security Infrastructure

## Contenu:

### Definition and Purpose of Security Architecture

- Security Architecture Components
- Security Architecture in Modern Networks
- Security Design Principles

### Components of Security Infrastructure

- Layers of Security Infrastructure - Physical, Network, Application and Data
- Infrastructure Components: Endpoints, Servers, Data Centers, and Cloud Environments
- Core Security Technologies: Firewalls, VPNs,IDS/IPS, IAM
- Design Case Study Activity 1: Migrating from Flat Network to Layered Design
- Design case Study Activity 2: Securing the Edge
- Design case Study Activity 3: Micro-Segmentation in a Virtualized Data Center
- Design case Study Activity 4: Endpoint and Insider Threat Response

### Security Design Principles

- Least Privileges and Zero Trust Models
- Defense-in-Depth and Multi-Layered Security Approaches
- Role of Encryption and Data -Integrity in Security Design
- Security by Design: Embedding Security in Development Lifecycles
- Visibility and Observability of Network Activities
- Design Practice Activity 1: Zero Trust Migration for Legacy Access Control
- Design Practice Activity 2: Designing Resilient Perimeter Security for a Hybrid Workforce
- Design Practice Activity 3: Secure Segmentation of Multi-Tenant Infrastructure
- Design Practice Activity 4: Business Continuity-Driven Security Design

### Security and Design Frameworks

- MITRE ATTACK Framework
- Common Attack Pattern Enumeration and Classification
- NIST Risk Management Framework
- Secure Access Service Edge (SASE)

### Compliance and Regulatory Requirements

- Regulatory Compliance for Security Designs
- Compliance Monitoring and Reporting

### Security Approaches to Protect Against Threats

- Endpoint and Client Device Security
- Identity and Access Management

### VPN and Tunneling Solutions

- Remote Access VPN
- WAN Connectivity
- SD-WAN and Cloud-Based Tunnels
- Design Practice Activity 1: Zero Trust Remote Access for Financial Analysts
- Design Practice Activity 2: Hybrid WAN Architecture for a Global Retail Chain
- Design Practice Activity 3: Cloud-First Strategy with Secure SD-WAN

### Secure Infrastructure Management and Control Planes

- Network Management Security
- Control Plane Security

### Nextgen Firewalls

- Differences between Traditional Firewalls and NGFWs
- NGFW Advanced Features
- Firewalls in SaaS Security
- Firewalls in Multi-Cloud and Data Center Security
- Design Practice Activity 1: Redefining Branch Security with Application Control
- Design Practice Activity 2: Malware Lateral Movement in the Data Center
- Design Practice Activity 3: Enforcing Compliance and Secure Segmentation

### Web Application Firewall (WAF)

- Web Application Security
- Integration of Web Application and API Protection (WAAP) with Content Delivery Networks (CDNs)

### IPS/IDS Deployment

- Key Features of IDS/IPS
- IDS/IPS Best Practices
- Design Practice Activity 1: IPS Design for a Financial Data Center
- Design Practice Activity 2: IPS Protection of Hybrid Workforce
- Design Practice Activity 3: Securing OT with IDS/IPS

### Host-Based Firewalls and Distributed Firewalls

- Host-Based Firewalls for Securing Endpoints
- Distributed Firewalls for Cloud-Native and Microservice Environments

### Security Solutions Based on Application and Flow Data

- Application Firewalls

### Emerging Technologies in Application Security

- Generative Artificial Intelligence and Machine Learning
- Quantum Computing Security Impacts

### SOC Tools for Incident Handling and Response

- SIEM Solutions Design
- SOAR Systems
- Network Observability
- eBPF ( extended Berkeley Packet Filters)

### Modify Design to Mitigate Risk

- Risk Management Frameworks
- Compensating Controls
- SAFE Framework
- Design Practice Activity 1: Selecting a Framework for a Government Contractor Network
- Design Practice Activity 2: Designing Security Capabilities Using Cisco SAFE Framework
- Design Practice Activity 3: Implementing Compensating Controls in a Legacy Banking System

### Incident-Driven Security Adjustments

- Post-Incident Response and Recovery
- Design Practice Activity 1: Recovery from Advanced Persistent Threat (APT)
- Design Practice Activity 2: Designing a DDoS Recovery and Resilience Strategy for Internet Edge
- Design Practice Activity 3: Mitigating and Recovering from a Framework
- Design Practice Activity 4: Incident response Design for Insider-Driven data Breach

### DevSecOps Integration

- Continuous Integration/Continuous Delivery (CI/CD) Pipeline Security
- Automated Vulnerability Scanning
- API Security

### Secure Automated Workflows and Pipelines

- Automated Security Testing for Continuous Compliance
- Integrating DevSecOps Workflows with AI/ML for Enhanced Security Posture
- Security Design and AI Task 1: Threat Modeling with AI Assistance
- Security Design and AI Task 2: Secure Architecture Review
- Security Design and AI Task 3: AI-Assisted Secure Code Review

- Two-Factor Authentication and Cisco Duo
- Email Security
- Passwordless Authentication Technologies and Methodologies
- Passwordless Authentication User Experience
- Passwordless Authentication Implementation Changes

#### Modify the Security Architecture to Meet Technical Requirements

- Security for Hybrid Workers
- IoT Security Design
- SaaS Security
- Multi-Cloud and Data Center Security
- Design Practice Activity 1: Securing IoT Infrastructure in a Smart Hospital
- Design Practice Activity 2: Building a Secure SaaS Ecosystem
- Design Practice Activity 3: Designing Resilient Security in a Multi-Cloud Environment

#### Network Access Security

- 802.1x for User Authentication for Network Access
- MAC Authentication Bypass
- Web Authentication
- Design Practice Activity 1: Phased Deployment of 802.1X in a Multi-Building Enterprise
- Design Practice Activity 2: MAB and Endpoint Profiling in an IoT-Rich Environment
- Design Practice Activity 3: WebAuth for BYOD and Guest Access at a Financial Institution

- SSL Offloading and Decryption
- Data Loss Prevention (DLP)
- Endpoint Security in Application Data Flows
- DNS Security
- Design Practice Activity 1: Designing a Resilient Web Application Firewall
- Design Practice Activity 2: Secure SSL/TLS Decryption Strategy in a Privacy-Conscious Environment
- Design Practice Activity 3: DNS-Layer Defense Integration in a Remote and Hybrid Workforce
- Design Practice Activity 4: Designing Endpoint Security Enforcement in a Hybrid Enterprise

#### Security for Cloud-Native Applications, Microservices, and Containers

- Microservices Security and Segmentation
- Containers and Kubernetes Security
- Serverless Architecture

- Security Design and AI Task 4: Designing a Secure Login System
- Security Design and AI Task 5: Writing a Security Policy with ChatGPT
- Security Design and AI Task 6: AI as an Adversary: Red Team Scenario Design
- Security Design and AI Task 7: Privacy by Design - Data Flow Analysis
- Security Design and AI Task 8: Risk Assessment Report with AI Help
- Security Design and AI Task 9: Designing Security Awareness Campaign
- Security Design and AI Task 10: Incident Response Plan Simulation

#### AI's Role in Securing Infrastructure

- AI-Driven Threat Detection and Response
- Infrastructure as Code (IAC) for Security
- Security Telemetry and Monitoring

#### Labs:

- There are no labs associated with this training.

## Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

#### Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "booking form" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via [moncompteformation.gouv.fr](http://moncompteformation.gouv.fr).

#### Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur [globalknowledge.fr/handicap](http://globalknowledge.fr/handicap)
- Le Règlement intérieur est disponible sur [globalknowledge.fr/reglement](http://globalknowledge.fr/reglement)