

Designing Cisco Security Infrastructure v1.0 (SDSI)

Cisco Authorized Training · Applied Technology Academy

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

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	5 Days	Cisco CCNA	\$125,00	Yes

Course Overview

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

Course Outline

- Definition and Purpose of Security Architecture
- Components of Security Infrastructure
- Security Design Principles
- Security and Design Frameworks
- Compliance and Regulatory Requirements
- Security Approaches to Protect Against Threats
- Modify the Security Architecture to Meet Technical Requirements
- Network Access Security
- VPN and Tunneling Solutions
- Secure Infrastructure Management and Control Planes
- Nextgen Firewalls
- Web Application Firewall (WAF)
- IPS/IDS Deployment
- Host-Based Firewalls and Distributed Firewalls
- Security Solutions Based on Application and Flow Data
- Security for Cloud-Native Applications, Microservices, and Containers
- Emerging Technologies in Application Security
- SOC Tools for Incident Handling and Response
- Modify Design to Mitigate Risk
- Incident-Driven Security Adjustments
- DevSecOps Integration
- Secure Automated Workflows and Pipelines
- AI's Role in Securing Infrastructure

Intended Audience

- Security Engineer
- Network Engineer
- Network Designer
- Network Administrator
- Systems Engineer
- Consulting Systems Engineer
- Technical Solutions Architect
- Cisco Integrators/Partners
- Network Manager
- Cisco integrators and partners

Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- Cisco CCNP Security or equivalent knowledge
- Familiarity with Microsoft Windows Operating Systems
- Familiarity with the Cisco Security portfolio

Follow-On Courses

- Implementing and Operating Cisco Security Core Technologies (SCOR)
- Implementing and Configuring Cisco Identity Services Engine Training (SISE)

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.