Current Technologies
Computer Learning Centers

cisco Partner
Platinum Learning

Designing Cisco Security Infrastructure (SDSI) v1.0

WHERE GREAT TRAINING HAPPENS EVERYDAY!

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Designing Cisco Security Infrastructure (SDSI) v1.0

Course Duration

5 days

Course Price

$4,400.00
45 CLCs

Methods of Delivery

In-Person ILT
Virtual ILT
Onsite ILT

About this Class

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. This training prepares you for the 300-745 SDSI v1.0 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 training also earns you 41 Continuing Education (CE) credits toward recertification.

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Designing Cisco Security Infrastructure (SDSI) v1.0

How you will benefit

This class will help you:

- Gain hands-on experience of security architecture design
- Qualify for professional and expert-level security job roles
- Prepare for the 300-745 SDSI v1.0 exam
- Earn 41 CE credits toward recertification

Why Attend with Current Technologies CLC

- Our Instructors are the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The job roles best suited to the material in this course are:

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

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

Designing Cisco Security Infrastructure (SDSI) v1.0

Objectives

After taking 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

Designing Cisco Security Infrastructure (SDSI) v1.0

Objectives

After taking this course, you should be able to:

- 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

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Designing Cisco Security Infrastructure (SDSI) v1.0

Course Outline

- Module 1: Definition and Purpose of Security Architecture
- Module 2: Components of Security Infrastructure
- Module 3: Security Design Principles
- Module 4: Security and Design Frameworks
- Module 5: Compliance and Regulatory Requirements
- Module 6: Security Approaches to Protect Against Threats
- Module 7: Modify the Security Architecture to Meet Technical Requirements
- Module 8: Network Access Security
- Module 9: VPN and Tunneling Solutions
- Module 10: Secure Infrastructure Management and Control Planes
- Module 11: Nextgen Firewalls
- Module 12: Web Application Firewall (WAF)
- Module 13: IPS/IDS Deployment
- Module 14: Host-Based Firewalls and Distributed Firewalls
- Module 15: Security Solutions Based on Application and Flow Data
- Module 16: Security for Cloud-Native Applications, Microservices, and Containers
- Module 17: Emerging Technologies in Application Security
- Module 18: SOC Tools for Incident Handling and Response
- Module 19: Modify Design to Mitigate Risk
- Module 20: Incident-Driven Security Adjustments
- Module 21: DevSecOps Integration
- Module 22: Secure Automated Workflows and Pipelines
- Module 23: AI's Role in Securing Infrastructure