Current Technologies
Computer Learning Centers

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

CISCO Partner
Platinum Learning

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Designing Cisco Security Infrastructure (SDSI) v1.0

Designing Cisco Security Infrastructure (SDSI) v1.0

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.

How you'll 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

Course Duration

5 days

Course Price

$4,400.00 or 45 CLCs

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Why Attend with Current Technologies CLC

- Our Instructors are in 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 primary audience for this course is as follows:

- 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

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

LAB OUTLINE

There are no labs associated with this training.