SDSI

Designing Cisco Security Infrastructure

40 horas | Profissional | Cisco

Cisco Continuing Education Credits

41 CE Credits

INTRODUÇÃO

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

OBJETIVO DO CURSO

Identify fundamental concepts of security architecture

Identify layers of security infrastructure and core security technologies

Explain security design principles

Identify security design and management frameworks

Explain regulatory compliance in security design

Identify tools for detection and response to security incidents

Explain strategies to modify traditional security architectures for modern enterprise networks

Implement secure network access methods (802.1X, MAB, web-based authentication)

Describe security technologies for enterprise WAN connections

Compare methods to secure network management and control plane traffic

Compare traditional firewalls vs. NGFWs

Explain web application firewalls (WAFs)

Describe IDS/IPS deployment best practices

Explain endpoint and cloud-native service protection

Discuss security for application data and data in transit

Identify security solutions for cloud-native applications and containers

Explain AI role in threat detection and response

Identify tools for detection and response to security incidents

Describe frameworks to mitigate security risks

Identify DevSecOps integrations

Discuss how to ensure automated services are secure

PÚBLICO-ALVO

Cisco and Partner Systems Engineers, Customer Network and Infrastructure Engineers, Customer Security/NOC Engineers

PRÉ-REQUISITOS

No formal prerequisites. Recommended: CCNP Security or equivalent, familiarity with Windows OS and Cisco Security portfolio.

CONTEÚDO PROGRAMÁTICO

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

Next-Gen Firewalls

Web Application Firewall (WAF)

IPS/IDS Deployment

Host-Based 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

Lab Outline

There are no labs associated with this training.