SCAZT

Designing and Implementing Secure Cloud Access for Users and Endpoints

40 horas | Profissional | Cisco

Cisco Continuing Education Credits

40 CE Credits

INTRODUÇÃO

The SCAZT training teaches you the skills for designing and implementing cloud security architecture, user and device security, network and cloud security, cloud application and data security, cloud visibility and assurance, and responding to cloud threats.

OBJETIVO DO CURSO

Compare NIST, CISA, and DISA security frameworks

Describe the Cisco Security Reference Architecture

Describe commonly deployed use cases and capabilities within an integrated security architecture

Describe the Cisco SAFE architecture

Review certificate-based authentication for users and devices

Enable Cisco Duo MFA to protect applications

Install Cisco Duo and implement MFA on remote access VPN

Configure endpoint compliance

Review SSO using SAML or OpenID Connect with Cisco Duo

Describe Cisco SD-WAN on-box threat prevention and content filtering

Describe Cisco Umbrella SIG features including DNS Security, CDFW, and IPS

Introduce reverse proxy for internet-facing application protection

Explore Cisco ThousandEyes capabilities for SD-WAN monitoring

Introduce Cisco Secure Firewall platforms and capabilities

Demonstrate web application firewall understanding

Demonstrate Cisco Secure Workload capabilities and deployment

Describe common cloud attack tactics and mitigation strategies

Describe multicloud security requirements

Introduce cloud visibility and assurance tools

Describe Cisco Secure Network Analytics and Security Analytics and Logging

Describe Cisco Attack Surface Management

Demonstrate knowledge of responses to cloud threats

Demonstrate automation for cloud threat detection and response

PÚBLICO-ALVO

Network Engineers, Network Security Engineers, Network Architects, Sales/Presales Engineers

PRÉ-REQUISITOS

No formal prerequisites. Recommended: enterprise routing/switching, WAN networking, Cisco SD-WAN, public cloud services, VPN technologies, and Cisco security solutions knowledge.

CONTEÚDO PROGRAMÁTICO

Course Outline

Certificate-Based User and Device Authentication

Cisco Duo MFA for Application Protection

Cisco Duo with AnyConnect VPN

Cisco ISE Endpoint Compliance Services

SSO using SAML or OpenID Connect

Reverse Proxy

Cisco SD-WAN Security Content Filtering

Cisco SD-WAN to Cisco Umbrella SIG Integration

Cisco Umbrella Cloud Access Security Broker

Security Policies for Remote Access VPN

Cisco Secure Access

Cisco Secure Firewall

Web Application Firewall

Cisco Secure Workload Deployments and Policy

Multicloud Security Policies

Cloud Security Attacks and Mitigations

Cloud Visibility and Assurance

Cisco Secure Network Analytics

Cisco XDR

Cisco Attack Surface Management

Industry Security Frameworks

Cisco Security Reference Architecture

Cisco SAFE Architecture

Cisco SD-WAN with ThousandEyes

Automation of Cloud Policy

Response to Cloud Threats

Lab Outline

Use Cisco Duo MFA to Protect the Splunk Application

Implement Cisco Duo Authentication Proxy MFA for Remote Access

Compliance-Based Access

Implement Web Security

Deploy DIA Security with Unified Security Policy

Configure Cisco Umbrella DNS Policies

Deploy Cisco Umbrella SIG

Implement CASB Security

Configure Remote Access VPN on Cisco Secure Firewall

Configure Cisco Secure Firewall Policies

Explore Cisco Secure Workload

Explore Cisco Secure Network Analytics

Explore Cisco XDR Incident Response Tasks