Cisco Security Essentials: Access, Network, and XDR

This Cisco Security Essentials course prepares IT professionals to defend modern enterprise infrastructure using Zero Trust principles and consistent policy enforcement. Dive deep into the Cisco Secure Reference Architecture (SRA) to explore PKI foundations, identity-based access control with Cisco ISE and Duo, and integrated cloud security. This course covers advanced network protection, including SD-WAN integration with Umbrella and workload security across multi-cloud environments. You'll also get comfortable with XDR orchestration by leveraging Talos threat intelligence and using ThousandEyes for end-to-end visibility. Once you're done with this course, you'll have the expertise to design and deploy a resilient security fabric across any enterprise landscape.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Exploring Security Frameworks: Part 1

Security Framework Overview

Common Security Frameworks

The NIST Framework

The NIST Core Functions

Challenge

Exploring Security Frameworks: Part 2

Introduction

The CISA Framework

The DISA Framework

DISA RMF Implementation

DISA STIGs, Tools, and Benefits

Comparing the Different Frameworks

Challenge

Cisco SRA: User and Device Security Intro

Introduction

Authentication Overview

Zero Trust

Assessing Risks - Users

Assessing Risks - Devices

Challenge

Cisco SRA: User and Device Security Measures

Introduction

Security Measures

Discovering Cisco Duo

Secure Access Service Edge

Challenge

Certificate-Based Authentication Foundations

Introduction

PKI

Certificates

User vs Device Certificates

Exploring Windows Certificate Manager

Challenge

Certificate-Based Access Control Using Cisco ISE

Introduction

Certificates and Identity Trust in Cisco ISE

Cisco ISE Certificate Authority Services

Cisco ISE BYOD Certificate Services

Certificate Trust, Status, and Integrations

Common PKI Problems in Cisco ISE

Challenge

Cisco DUO Application Protection

Introduction

Identity Brokering with Duo

Adaptive Access Polices

Enabling Duo Passport

Protecting a SaaS Application

Enabling Duo Central

Verify Access to Duo Central

Verify Seamless Access with Duo Passport

Challenge

802.1X Certificate-Based Network Access

Introduction

802.1X Fundamentals

EAP Protocol Overview

802.1X Authentication Exchange

EAP Authentication Methods

Challenge

SRA Use Cases: Common Identity

Introduction

Terms Review

Common ID in the SRA

Common ID in Action

From Endpoints to Cloud

Benefits of Common Identity

Challenge

Identity-Aware Application Access

Introduction

Exploring Single Sign-On and SAML

Using Single Sign-On with SAML and OpenID Connect

Cisco Duo as a Cloud-Based SSO IdP

Where Identity Enforcement Happens

Reverse Proxy and Forward Proxy Fundamentals

Reverse Proxy Implementation for Application Protection

Challenge

Using DUO with AnyConnect VPN

Introduction

Getting Connected and Logged in to DUO

AD Sync and SSO

Adding Trusted Endpoints

Configure VPN in Duo

User Enrollment

Challenge

Secure Remote Access VPN Policies

Introduction

Remote VPN Security on Secure Firewall

SD-WAN Remote VPN Security Policies

Remote Access VPN Implementation

Verify and Troubleshoot VPN Configuration

Challenge

SRA Use Cases: Zero Trust Network Access

Introduction

ZTNA Overview

MFA with DUO

Device Profiling

ZTNA Challenges

Challenge

Cisco SRA: Network Security

Introduction

On Prem vs. Cloud Edge

Network Security Components

Industrial IoT Threat Defense

Challenge

Cisco SRA: Advanced Network Security

Introduction

Secure Access Service Edge Architecture

Network Security in Varying Environments

Microservices

Container Security

Challenge

Cisco SRA: Workload Application and Data Security

Introduction

Application Workloads

From VMs to Serverless

Challenges Surrounding Workloads

Challenge

Cisco SRA: Cisco Secure Workload

Introduction

Why Workload Security Matters

Cisco Secure Workload

Exploring Cisco Secure Workload

Challenge

SD-WAN Content Filtering

Introduction

SD-WAN Content Filtering Overview

URL Filtering and TLS/SSL Decryption

Verify and Modify Security Policy

Challenge

Integrate SD-WAN with Cisco Umbrella

Introduction

Cisco Umbrella SIG Architecture and Components

How Cisco SD-WAN Connects to Secure Internet Gateway

DNS-Layer Protection with Cisco Umbrella

Cloud-Delivered Firewall and Intrusion Prevention

Web Security with Cisco Umbrella

Challenge

Implement Umbrella DNS with SD-WAN

Introduction

Pre-Deployment Lab Verification

Umbrella DNS with Unified Policy

Configure and Verify Umbrella DNS Policy

Advanced Filtering Options

Challenge

Implement Umbrella SIG with SD-WAN

Introduction

Pre-Deployment Lab Verification

Integrate Branch Internet Access with Umbrella SIG

Steer Branch Internet Traffic to Umbrella SIG

Applying and Validating Web Security Policy in Cisco Umbrella

Challenge

Understand Umbrella Access Security Broker

Introduction

Securing SaaS and Shadow IT with Cisco Umbrella CASB

Cloud Application Control with Umbrella CASB

Cloud Data Protection with Umbrella CASB

Implementing Tenant-Based CASB Controls

Challenge

Cisco ThousandEyes Fundamentals

Introduction

ThousandEyes Overview

ThousandEyes Core Benefits

ThousandEyes Architecture Overview

ThousandEyes Agent Types and Vantage Points

ThousandEyes Test Types and Layers

Challenge

Integrate Cisco SD-WAN with ThousandEyes

Introduction

ThousandEyes Visibility in SD-WAN Environments

ThousandEyes Deployment Models

Supported Platforms and Deployment Benefits

WEEK 2

ThousandEyes Container Architecture

Deploying ThousandEyes Enterprise Agents at Scale

Challenge

Cisco SRA: XDR Toolset

Introduction

XDR Toolset Overview

Cisco XDR

Vulnerability Management

Secure Analytics

Cisco Secure Client

Talos Incident Response

Challenge

SRA Use Cases: XDR Telemetry and Orchestration

Introduction

Cisco SecureX

Cisco XDR

XDR Integrations

XDR Orchestration

XDR Control Center

XDR Incidents

XDR Investigate

XDR Threat Intelligence

Challenge

SRA Use Cases: Converged Multicloud Policy

Introduction

Multicloud Policy Overview

Implementing Multicloud Security

Policy Orchestration

Policy Enforcement

Challenge

SRA Use Cases: SASE Integration

Introduction

Understanding SASE

SASE Architecture

Key Components of SASE

Challenge

Cisco SRA: Talos

Introduction

Security Reference Architecture Overview

The Role of Threat Intelligence

What is Cisco Talos?

Talos in Cisco XDR

Use Cases and Other Benefits

Exploring Cisco Talos

Challenge

Explore the Cisco SAFE Architecture

Introduction

Understanding the Cisco SAFE Model

SAFE Key and Places in the Network

SAFE Security Domains and Capability Diagrams

SAFE Phases of Implementation

Challenge

SD-WAN Direct Internet Access

Introduction

Secure Direct Internet Access

Designing and Deploying Unified Security Policies

Securing Direct Internet Access with Unified Security Policies

Challenge

Last updated 6.10.2026