Current Technologies
Computer Learning Centers

CISCO Partner
Platinum Learning

Implementing and Operating Cisco Security Core Technologies (SCOR) V2.0

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Implementing and Operating Cisco Security Core Technologies (SCOR) V2.0

Course Duration

5 Days

Course Price

$4,295.00
43 CLCs

Methods of Delivery

In-Person ILT
Virtual ILT
Onsite ILT

About this Class

The Implementing and Operating Cisco Security Core Technologies (SCOR) v2.0 training helps you gain the skills and technologies needed to implement core Cisco security solutions. This training will prepare you to provide advanced threat protection against cybersecurity attacks and prepare you for senior-level security roles. This training prepares you for the 350-701 SCOR v1.0 exam. If passed, you earn the Cisco Certified Specialist - Security Core certification and satisfy the core exam requirement for the Cisco Certified Network Professional (CCNP) Security and Cisco Certified Internetwork Expert (CCIE) Security certifications. This training also earns you 64 Continuing Education (CE) credits towards recertification.

Implementing and Operating Cisco Security Core Technologies (SCOR) V2.0

How you will benefit

This class will help you:

- Gain hands-on experience implementing core security technologies and learn best practices using Cisco security solutions
- Qualify for professional and expert-level security job roles
- Prepare for the 350-701 SCOR v1.0 exam
- Earn 64 CE credits towards 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:

- Security Engineer
- Network Engineer
- Network Designer
- Network Administrator
- Systems Engineer
- Consulting Systems Engineer
- Technical Solutions Architect
- Network Manager
- Cisco Integrators and Partners

Implementing and Operating Cisco Security Core Technologies (SCOR) V2.0

Objectives

After taking this course, you should be able to:

- Describe information security concepts and strategies within the network
- Describe security flaws in the transmission protocol/internet protocol (TCP/IP) and how they can be used to attack networks and hosts
- Describe network application-based attacks
- Describe how various network security technologies work together to guard against attacks
- Implement access control on Cisco Secure Firewall Adaptive Security Appliance (ASA)
- Deploy Cisco Secure Firewall Threat Defense basic configurations
- Deploy Cisco Secure Firewall Threat Defense IPS, malware, and fire policies
- Deploy Cisco Secure Email Gateway basic configurations
- Deploy Cisco Secure Email Gateway policy configurations
- Describe and implement basic web content security features and functions provided by Cisco Secure Web Appliance
- Describe various attack techniques against the endpoints
- Describe Cisco Umbrella® security capabilities, deployment models, policy management, and Investigate console
- Provide basic understanding of endpoint security and be familiar with common endpoint security technologies
- Describe Cisco Secure Endpoint architecture and basic features
- Describe Cisco Secure Network Access solutions
- Describe 802.1X and extensible authentication protocol (EAP) authentication
- Configure devices for 802.1X operations
- Introduce VPNs and describe cryptography solutions and algorithms

Implementing and Operating Cisco Security Core Technologies (SCOR) V2.0

Objectives

- Describe Cisco secure site-to-site connectivity solutions
- Deploy Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-based point-to-point IPsec VPNs
- Configure point-to-point IPsec VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense
- Describe Cisco secure remote access connectivity solutions
- Deploy Cisco secure remote access connectivity solutions
- Provide an overview of network infrastructure protection controls
- Examine various defenses on Cisco devices that protect the control plane
- Configure and verify Cisco IOS software layer 2 data plane controls
- Configure and verify Cisco IOS software and Cisco ASA layer 3 data plane controls
- Examine various defenses on Cisco devices that protect the management plane
- Describe the baseline forms of telemetry recommended for network infrastructure and security devices
- Describe deploying Cisco Secure Network Analytics
- Describe basics of cloud computing and common cloud attacks
- Describe how to secure cloud environment
- Describe the deployment of Cisco Secure Cloud Analytics
- Describe basics of software-defined networks and network programmability

Implementing and Operating Cisco Security Core Technologies (SCOR) V2.0

Course Outline

Module 1: Network Security Technologies

Module 2: Cisco Secure Firewall ASA Deployment

Module 3: Cisco Secure Firewall Threat Defense Basics

Module 4: Cisco Secure Firewall Threat Defense IPS, Malware, and File Policies

Module 5: Cisco Secure Email Gateway Basics

Module 6: Cisco Secure Email Policy Configuration

Module 7: Cisco Secure Web Appliance Deployment

Module 8: VPN Technologies and Cryptography Concepts

Module 9: Cisco Secure Site-to-Site VPN Solutions

Module 10: Cisco IOS VTI-Based Point-to-Point IPsec VPNs

Module 11: Point-to-Point IPsec VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense

Module 12: Cisco Secure Remote-Access VPN Solutions

Module 13: Remote-Access SSL VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense

Module 14: Describing Information Security Concepts

Module 15: Describe Common TCP/IP Attacks

Module 16: Describe Common Network Application Attacks

Module 17: Common Endpoint Attacks

Implementing and Operating Cisco Security Core Technologies (SCOR) V2.0

Course Outline

Module 18: Cisco Umbrella Deployment

Module 19: Endpoint Security Technologies

Module 20: Cisco Secure Endpoint

Module 21: Cisco Secure Network Access Solutions

Module 22: 802.1X Authentication

Module 23: 802.1X Authentication Configuration

Module 24: Network Infrastructure Protection

Module 25: Control Plane Security Solutions

Module 26: Layer 2 Data Plane Security Controls

Module 27: Layer 3 Data Plane Security Controls

Module 28: Management Plane Security Controls

Module 29: Traffic Telemetry Methods

Module 30: Cisco Secure Network Analytics Deployment

Module 31: Cloud Computing and Cloud Security

Module 32: Cloud Security

Module 33: Cisco Secure Cloud Analytics Deployment

Module 34: Software-Defined Networking

Implementing and Operating Cisco Security Core Technologies (SCOR) V2.0

Lab Outline

- Lab 1: Configure Network Settings and NAT on Cisco Secure Firewall ASA
- Lab 2: Configure Cisco Secure Firewall ASA Access Control Policies
- Lab 3: Configure Cisco Secure Firewall Threat Defense NAT
- Lab 4: Configure Cisco Secure Firewall Threat Defense Access Control Policy
- Lab 5: Configure Cisco Secure Firewall Threat Defense Discovery and IPS Policy
- Lab 6: Configure Cisco Secure Firewall Threat Defense Malware and File Policy
- Lab 7: Configure Listener, HAT, and RAT on Cisco Email Secure Email Gateway
- Lab 8: Configure Cisco Secure Email Policies
- Lab 9: Configure Proxy Services, Authentication, and HTTPS Decryption
- Lab 10: Enforce Acceptable Use Control and Malware Protection
- Lab 11: Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Lab 12: Configure Point-to-Point VPN between Cisco Secure Firewall Threat Defense Devices
- Lab 13: Configure Remote Access VPN on the Cisco Secure Firewall Threat Defense

Implementing and Operating Cisco Security Core Technologies (SCOR) V2.0

Lab Outline Cont.

- **Lab 14: Examine Cisco Umbrella Dashboard and DNS Security**
- **Lab 15: Examine Cisco Umbrella Secure Web Gateway and Cloud-Delivered Firewall**
- **Lab 16: Explore Cisco Umbrella CASB Functionalities**
- **Lab 17: Explore Cisco Secure Endpoint**
- **Lab 18: Perform Endpoint Analysis Using Cisco Secure Endpoint Console**
- **Lab 19: Explore File Ransomware Protection by Cisco Secure Endpoint Console**
- **Lab 20: Explore Secure Network Analytics v7.4.2**
- **Lab 21: Explore Global Threat Alerts Integration and ETA Cryptographic Audit**
- **Lab 22: Explore Cloud Analytics Dashboard and Operations**
- **Lab 23: Explore Secure Cloud Private and Public Cloud Monitoring**