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

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

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.

How you'll 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 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:

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

Course Duration
5 days
Course Price
$4,295.00 or 43 CLCs
Methods of Delivery
- Instructor Led
- Virtual ILT
- On-Site

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

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

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**
- **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**