Current Technologies
Computer Learning Centers

☎ +1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

CISCO Partner
Platinum Learning

WHERE GREAT TRAINING HAPPENS EVERYDAY!

IMPLEMENTING AND OPERATING CISCO SECURITY CORE TECHNOLOGIES (SCOR) V1.0

IMPLEMENTING AND OPERATING CISCO SECURITY CORE TECHNOLOGIES (SCOR) V1.0

The Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 course helps you prepare for the Cisco® CCNP® Security and CCIE® Security certifications and for senior-level security roles. In this course, you will master the skills and technologies you need to implement core Cisco security solutions to provide advanced threat protection against cybersecurity attacks. You will learn security for networks, cloud and content, endpoint protection, secure network access, visibility, and enforcements. You will get extensive hands-on experience deploying Cisco Firepower® Next-Generation Firewall and Cisco Adaptive Security Appliance (ASA) Firewall; configuring access control policies, mail policies, and 802.1X Authentication; and more. You will get introductory practice on Cisco Stealthwatch® Enterprise and Cisco Stealthwatch Cloud threat detection features.

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
- Prepare for the Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) exam
- Qualify for professional and expert-level security job roles
- Earn 64 CE credits toward 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: Describing Information Security Concepts*

- Information Security Overview
- Assets, Vulnerabilities, and Countermeasures
- Managing Risk
- Vulnerability Assessment
- Understanding Common Vulnerability Scoring System (CVSS)

Module 2: Describing Common TCP/IP Attacks*

- Legacy TCP/IP Vulnerabilities
- IP Vulnerabilities
- Internet Control Message Protocol (ICMP) Vulnerabilities

Module 3: Describing Common Network Application Attacks*

- Password Attacks
- Domain Name System (DNS)-Based Attacks
- DNS Tunneling

Module 4: Describing Common Endpoint Attacks*

- Buffer Overflow
- Malware
- Reconnaissance Attack

Module 5: Describing Network Security Technologies

- Defense-in-Depth Strategy
- Defending Across the Attack Continuum
- Network Segmentation and Virtualization Overview

Module 6: Deploying Cisco ASA Firewall

- Cisco ASA Deployment Types
- Cisco ASA Interface Security Levels
- Cisco ASA Objects and Object Groups

Module 7: Deploying Cisco Firepower Next-Generation Firewall

- Cisco Firepower NGFW Deployments
- Cisco Firepower NGFW Packet Processing and Policies
- Cisco Firepower NGFW Objects

Module 8: Deploying Email Content Security

- Cisco Email Content Security Overview
- Simple Mail Transfer Protocol (SMTP) Overview
- Email Pipeline Overview

Module 9: Deploying Web Content Security

- Cisco Web Security Appliance (WSA) Overview
- Deployment Options
- Network Users Authentication

Module 10: Deploying Cisco Umbrella*

- Cisco Umbrella Architecture
- Deploying Cisco Umbrella
- Cisco Umbrella Roaming Client

Module 11: Explaining VPN Technologies and Cryptography

- VPN Definition
- VPN Types
- Secure Communication and Cryptographic Services

Module 12: Introducing Cisco Secure Site-to-Site VPN Solutions

- Site-to-Site VPN Topologies
- IPsec VPN Overview
- IPsec Static Crypto Maps

Module 13: Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs

- Cisco IOS VTIs
- Static VTI Point-to-Point IPsec Internet Key Exchange (IKE) v2 VPN Configuration

Module 14: Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW

- Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
- Cisco ASA Point-to-Point VPN Configuration
- Cisco Firepower NGFW Point-to-Point VPN Configuration

Module 15: Introducing Cisco Secure Remote Access VPN Solutions

- Remote Access VPN Components
- Remote Access VPN Technologies
- Secure Sockets Layer (SSL) Overview

Module 16: Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW

- Remote Access Configuration Concepts
- Connection Profiles
- Group Policies

Module 17: Explaining Cisco Secure Network Access Solutions

- Cisco Secure Network Access
- Cisco Secure Network Access Components
- AAA Role in Cisco Secure Network Access Solution

Module 18: Describing 802.1X Authentication

- 802.1X and Extensible Authentication Protocol (EAP)
- EAP Methods
- Role of Remote Authentication Dial-in User Service (RADIUS) in 802.1X Communications

Module 19: Configuring 802.1X Authentication

- Cisco Catalyst® Switch 802.1X Configuration
- Cisco Wireless LAN Controller (WLC) 802.1X Configuration
- Cisco Identity Services Engine (ISE) 802.1X Configuration

Module 20: Describing Endpoint Security Technologies*

- Host-Based Personal Firewall
- Host-Based Anti-Virus
- Host-Based Intrusion Prevention System

Module 21: Deploying Cisco Advanced Malware Protection (AMP) for Endpoints*

- Cisco AMP for Endpoints Architecture
- Cisco AMP for Endpoints Engines
- Retrospective Security with Cisco AMP

Module 22: Introducing Network Infrastructure Protection*

- Identifying Network Device Planes
- Control Plane Security Controls
- Management Plane Security Controls

Module 23: Deploying Control Plane Security Controls*

- Infrastructure ACLs
- Control Plane Policing
- Control Plane Protection

Module 24: Deploying Layer 2 Data Plane Security Controls*

- Overview of Layer 2 Data Plane Security Controls
- Virtual LAN (VLAN)-Based Attacks Mitigation
- Spanning Tree Protocol (STP) Attacks Mitigation

Module 25: Deploying Layer 3 Data Plane Security Controls*

- Infrastructure Antispoofing ACLs
- Unicast Reverse Path Forwarding
- IP Source Guard

Module 26: Deploying Management Plane Security Controls*

- Cisco Secure Management Access
- Simple Network Management Protocol Version 3
- Secure Access to Cisco Devices

Module 27: Deploying Traffic Telemetry Methods*

- Network Time Protocol
- Device and Network Events Logging and Export
- Network Traffic Monitoring Using NetFlow

Module 28: Deploying Cisco Stealthwatch Enterprise*

- Cisco Stealthwatch Offerings Overview
- Cisco Stealthwatch Enterprise Required Components
- Flow Stitching and Deduplication

Module 29: Describing Cloud and Common Cloud Attacks**

- Evolution of Cloud Computing
- Cloud Service Models
- Security Responsibilities in Cloud

Module 30: Securing the Cloud*

- Cisco Threat-Centric Approach to Network Security
- Cloud Physical Environment Security
- Application and Workload Security

Module 31: Deploying Cisco Stealthwatch Cloud*

- Cisco Stealthwatch Cloud for Public Cloud Monitoring
- Cisco Stealthwatch Cloud for Private Network Monitoring
- Cisco Stealthwatch Cloud Operations

Module 32: Describing Software-Defined Networking (SDN*)

- Software-Defined Networking Concepts
- Network Programmability and Automation
- Cisco Platforms and APIs
- Basic Python Scripts for Automation

LAB OUTLINE

- **Lab 1: Configure Network Settings and NAT on Cisco ASA**
- **Lab 2: Configure Cisco ASA Access Control Policies**
- **Lab 3: Configure Cisco Firepower NGFW NAT**
- **Lab 4: Configure Cisco Firepower NGFW Access Control Policy**
- **Lab 5: Configure Cisco Firepower NGFW Discovery and IPS Policy**
- **Lab 6: Configure Cisco NGFW Malware and File Policy**
- **Lab 7: Configure Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security Appliance (ESA)**
- **Lab 8: Configure Mail Policies**
- **Lab 9: Configure Proxy Services, Authentication, and HTTPS Decryption**
- **Lab 10: Enforce Acceptable Use Control and Malware Protection**
- **Lab 11: Examine the Umbrella Dashboard**
- **Lab 12: Examine Cisco Umbrella Investigate**

- **Lab 13: Explore DNS Ransomware Protection by Cisco Umbrella**
- **Lab 14: Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel**
- **Lab 15: Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW**
- **Lab 16: Configure Remote Access VPN on the Cisco Firepower NGFW**
- **Lab 17: Explore Cisco AMP for Endpoints**
- **Lab 18: Perform Endpoint Analysis Using AMP for Endpoints Console**
- **Lab 19: Explore File Ransomware Protection by Cisco AMP for Endpoints Console**
- **Lab 20: Explore Cisco Stealthwatch Enterprise v6.9.3**
- **Lab 21: Explore Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0**
- **Lab 22: Explore the Cisco Cloudlock Dashboard and User Security**
- **Lab 23: Explore Cisco Cloudlock Application and Data Security**
- **Lab 24: Explore Cisco Stealthwatch Cloud**
- **Lab 25: Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors**