Implementing and Operating Cisco Security Core Technologies (SCOR)

Course Duration: 5 Days
Exam Reference: 350-701 SCOR

Course Overview

The Cisco SCOR 350-701 course covers core security technologies, including network security, cloud security, content security, endpoint protection, secure network access, visibility, and enforcement. It prepares professionals for roles in security operations and engineering, and is the core exam for the CCNP Security certification path.

This training also lays the foundation for understanding Cisco's security infrastructure and helps prepare for Cisco Certified CyberOps Professional and CCIE Security certifications.

Prerequisites

- Familiarity with network fundamentals
- Understanding of IP addressing and routing
- Basic knowledge of security concepts
- Recommended: CCNA or equivalent knowledge

Course Objectives

- Implement and manage core security technologies
- Configure and troubleshoot secure network infrastructure
- Secure access using Cisco Identity Services Engine (ISE)
- Implement firewall, VPN, and intrusion prevention systems
- Use Cisco cloud and email/web security solutions
- Monitor and respond to security incidents using Cisco tools

APPLIED TECHNOLOGY ACADEMY

Contact Us

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

Implementing and Operating Cisco Security Core Technologies (SCOR)

Course Outline

Module 1: Security Concepts

- Security principles and threats
- Cryptography fundamentals
- AAA concepts
- Security policies and frameworks

Module 2: Network Security

- Cisco ASA and NGFW firewall features
- Access Control Policies
- Intrusion prevention with Cisco NGIPS
- Network segmentation and zoning

Module 3: Secure Network Access

- Identity management and authentication
- Cisco Identity Services Engine (ISE)
- 802.1X and MAB authentication
- TrustSec and policy enforcement

Module 4: Endpoint Security

- Endpoint protection techniques
- Cisco AMP for Endpoints
- Malware protection and sandboxing
- EDR solutions overview

Module 5: Cloud Security

- Cloud security fundamentals
- Secure Internet Gateway (SIG)
- Cisco Umbrella features and policies
- Cloud access security broker (CASB) overview

Module 6: Content Security

- Email and web security challenges
- Cisco Secure Email Gateway

- Cisco Secure Web Appliance
- Filtering and malware defense

Module 7: Secure Network Management and Automation

- Network visibility tools and telemetry
- NetFlow, SNMP, and Syslog
- Cisco DNA Center security capabilities
- Automation and programmability with REST APIs

Module 8: VPN Technologies

- Site-to-site VPNs (IPsec)
- Remote access VPNs (SSL, IPsec IKEv2)
- Cisco ASA and FTD VPN configuration
- Troubleshooting VPN connectivity

Module 9: Threat Detection and Incident Response

- Security event monitoring
- Cisco SecureX and Secure Analytics
- Threat intelligence and threat hunting
- Incident response lifecycle and best practices