Implementing and Operating Cisco Security Core Technologies (SCOR) Training

Course: **00086**

Filter: **Beginner**

Duration: **5 days**

Category:: **Systems & Network Security**

Price: **2800,00 €**

About Course

SCOR Course Outline - 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 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. This course, including the self-paced material, helps prepare you to take the exam, Implementing and Operating Cisco Security Core Technologies (350-701 SCOR), which leads to the new CCNP Security, CCIE Security, and the Cisco Certified Specialist - Security Core certifications. To fully benefit from this course, you should have the following knowledge and skills: Skills and knowledge equivalent to those learned in Implementing and Administering Cisco Solutions (CCNA) v1.0 course Familiarity with Ethernet and TCP/IP networking; Working knowledge of the Windows operating system; Working knowledge of Cisco IOS networking and concepts; Familiarity with basics of networking security concepts; Security Engineer; Network Engineer; Network Designer; Network Administrator; Systems Engineer; Consulting Systems Engineer; Technical Solutions Architect; Cisco Integrators/Partners; Network Manager; Cisco integrators and partners; 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;

What you'll learn

- Describe network information security concepts and strategies
- Describe common TCP/IP, network application and endpoint attacks
- Describe how various network security technologies work together to protect against attacks
- Implement access control on the Cisco ASA appliance and the Cisco Firepower next-generation firewall
- Describe and implement the basic email content security features and functions provided by the Cisco Email Security Appliance
- Describe and implement the Web content security features and functions provided by the Cisco Web Security ApplianceDescribe the security capabilities of Cisco Umbrella
- Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco IOS VTI-based point-to-point IPsec VPNs and point-to-point IPsec VPNs over Cisco ASA and Cisco FirePower NGFWD Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802. 1X authentication and EAP authenticationProvide a basic understanding of endpoint security and describe the AMP architecture for endpoints and basic features
- Examine various defenses on Cisco devices that protect the control and management plane
- Configure and verify Cisco IOS Software Layer 2 and Layer 3 data plane controlsDescribe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions
- Describe the basics of cloud computing and common cloud computing attacks and how to secure the cloud computing environment

Pre-requisites

- None

Curriculum

Module 1: Describing Information Security Concepts

- Information Security Overview
- Managing Risk
- Vulnerability Assessment
- Understanding CVSS

Module 2: Describing Common TCP/IP Attacks

- Legacy TCP/IP Vulnerabilities
- IP Vulnerabilities
- ICMP Vulnerabilities
- TCP Vulnerabilities
- UDP Vulnerabilities
- Attack Surface and Attack Vectors
- Reconnaissance Attacks
- Access Attacks
- Man-In-The-Middle Attacks
- Denial of Service and Distributed Denial of Service Attacks
- Reflection and Amplification Attacks
- Spoofing Attacks
- DHCP Attacks

Module 3: Describing Common Network Application Attacks

- Password Attacks
- DNS-Based Attacks
- DNS Tunneling
- Web-Based Attacks
- HTTP 302 Cushioning
- Command Injections
- SQL Injections
- Cross-Site Scripting and Request Forgery
- Email-Based Attacks

Module 4: Describing Common Endpoint Attacks

- Buffer Overflow
- Malware
- Reconnaissance Attack
- Gaining Access and Control
- Gaining Access via Social Engineering
- Gaining Access via Web-Based Attacks
- Exploit Kits and Rootkits
- Privilege Escalation
- Post-Exploitation Phase
- Angler Exploit Kit

Module 5: Describing Network Security Technologies

- Defense-in-Depth Strategy
- Defending Across the Attack Continuum
- Network Segmentation and Virtualization Overview
- Stateful Firewall Overview
- Security Intelligence Overview
- Threat Information Standardization
- Network-Based Malware Protection Overview
- IPS Overview
- Next Generation Firewall Overview
- Email Content Security Overview
- Web Content Security Overview
- Threat Analytic Systems Overview
- DNS Security Overview
- Authentication, Authorization, and Accounting Overview
- Identity and Access Management Overview
- Virtual Private Network Technology Overview
- Network Security Device Form Factors Overview

Module 6: Deploying Cisco ASA Firewall

- Cisco ASA Deployment Types

- Cisco ASA Interface Security Levels
- Cisco ASA Objects and Object Groups
- Network Address Translation
- Cisco ASA Interface ACLs
- Cisco ASA Global ACLs
- Cisco ASA Advanced Access Policies
- Cisco ASA High Availability Overview

Module 7: Deploying Cisco Firepower Next-Generation Firewall

- Cisco Firepower NGFW Deployments
- Cisco Firepower NGFW Packet Processing and Policies
- Cisco Firepower NGFW Objects
- Cisco Firepower NGFW NAT
- Cisco Firepower NGFW Prefilter Policies
- Cisco Firepower NGFW Access Control Policies
- Cisco Firepower NGFW Security Intelligence
- Cisco Firepower NGFW Discovery Policies
- Cisco Firepower NGFW IPS Policies
- Cisco Firepower NGFW Malware and File Policies

Module 8: Deploying Email Content Security

- Cisco Email Content Security Overview
- SMTP Overview
- Email Pipeline Overview
- Public and Private Listeners
- Host Access Table Overview
- Recipient Access Table Overview
- Mail Policies Overview
- Protection Against Spam and Graymail
- Anti-virus and Anti-malware Protection
- Outbreak Filters
- Content Filters
- Data Loss Prevention
- Email Encryption

Module 9: Deploying Web Content Security

- Cisco WSA Overview
- Deployment Options
- Network Users Authentication
- HTTPS Traffic Decryption
- Access Policies and Identification Profiles
- Acceptable Use Controls Settings
- Anti-Malware Protection

Module 10: Deploying Cisco Umbrella

- Cisco Umbrella Architecture
- Deploying Cisco Umbrella
- Cisco Umbrella Roaming Client
- Managing Cisco Umbrella
- Cisco Umbrella Investigate Overview

Module 11: Explaining VPN Technologies and Cryptography

- VPN Definition
- VPN Types
- Secure Communication and Cryptographic Services
- Keys in Cryptography
- Public Key Infrastructure

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

- Site-to-Site VPN Topologies
- IPsec VPN Overview
- IPsec Static Crypto Maps
- IPsec Static Virtual Tunnel Interface
- Dynamic Multipoint VPN
- Cisco IOS FlexVPN

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

- Cisco IOS VTIs
- Static VTI Point-to-Point IPsec IKEv2 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
- 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
- Cisco ASA Remote Access VPN Configuration
- Cisco Firepower NGFW Remote Access VPN Configuration

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
- Cisco Identity Services Engine
- Cisco TrustSec

Module 18: Describing 802.1X Authentication

- 1X and EAP
- EAP Methods

- Role of RADIUS in 802.1X Communications
- RADIUS Change of Authorization

Module 19: Configuring 802.1X Authentication

- Cisco Catalyst Switch 802.1X Configuration
- Cisco WLC 802.1X Configuration
- Cisco ISE 802.1X Configuration
- Supplicant 802.1x Configuration
- Cisco Central Web Authentication

Module 20: Describing Endpoint Security Technologies

- Host-Based Personal Firewall
- Host-Based Anti-Virus
- Host-Based Intrusion Prevention System
- Application Whitelists and Blacklists
- Host-Based Malware Protection
- Sandboxing Overview
- File Integrity Checking

Module 21: Deploying Cisco AMP for Endpoints

- Cisco AMP for Endpoints Architecture
- Cisco AMP for Endpoints Engines
- Retrospective Security with Cisco AMP
- Cisco AMP Device and File Trajectory
- Managing Cisco AMP for Endpoints

Module 22: Introducing Network Infrastructure Protection

- Identifying Network Device Planes
- Control Plane Security Controls
- Management Plane Security Controls
- Network Telemetry
- Layer 2 Data Plane Security Controls

- Layer 3 Data Plane Security Controls

Module 23: Deploying Control Plane Security Controls

- Infrastructure ACLs
- Control Plane Policing
- Control Plane Protection
- Routing Protocol Security

Module 24: Deploying Layer 2 Data Plane Security Controls

- Overview of Layer 2 Data Plane Security Controls
- VLAN-Based Attacks Mitigation
- STP Attacks Mitigation
- Port Security
- Private VLANs
- DHCP Snooping
- ARP Inspection
- Storm Control
- MACsec Encryption

Module 25: Deploying Layer 3 Data Plane Security Controls

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