AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

Implementing and Operating Cisco Security Core Technologies
SCOR

Dauer	5 Tage
Kursstart/Status	Auf Anfrage 08:30-12:00 / 13:00-16:30
Kursort	Zürich
Kosten	CHF 4700.00 Lunch und Pausenverpflegungen inklusive. CLC einlösen: 43 für Kurs, plus CLC für MWST, plus CHF 2'645.00 Der Team Captain des Kunden muss die CLCs spätestens drei Arbeitstage vor Kursstart bei Cisco im Learning Locator eingelöst haben. Ist dies nicht der Fall, so wird die Kursteilnahme über normale Rechnungsstellung verrechnet.
Sprache	Deutsch
Dokumentation	Es wird immer die aktuellste Version geschult. Offizielle Cisco Kurs- und Labunterlagen in Englisch.

Überblick

Der Kurs Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 hilft Ihnen bei der Vorbereitung auf die Cisco CCNP Security- und CCIE Security-Zertifizierungen sowie auf Sicherheitsrollen auf höchster Ebene. In diesem Kurs erlernen Sie die Fähigkeiten und Technologien, die Sie zum Implementieren der wichtigsten Cisco Sicherheitslösungen benötigen, um erweiterten Schutz vor Cybersicherheitsangriffen zu bieten. Sie lernen Sicherheit für Netzwerke, Cloud und Inhalte, Endpoint protection, sicheren Netzwerkzugriff, Transparenz und enforcements. Sie erhalten umfassende praktische Erfahrung mit der Bereitstellung von Cisco Firepower Next-Generation Firewall und Cisco ASA Firewall, konfigurieren von Zugriffssteuerungsrichtlinien, E-Mail-Richtlinien und 802.1X-Authentifizierung; und mehr. Sie erhalten eine Einführung in die Bedrohungserkennungsfunktionen von Cisco Stealthwatch Enterprise und Cisco Stealthwatch Cloud.

Dieser Kurs, einschliesslich des Materials zum Selbststudium, bereitet Sie auf die Prüfung Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) vor. Daraus ergeben sich die neuen CCNP Security, CCIE Security und der Cisco Certified Specialist - Security Core - Zertifizierungen.

Voraussetzungen

- Fähigkeiten und Kenntnisse, die denen entsprechen, wie sie im Kurs Implementing and Administering Cisco Solutions (CCNA) v1.0 vermittelt werden
- Vertrautheit mit Ethernet- und TCP / IP-Netzwerken
- Grundkenntnisse des Windows-Betriebssystems
- Grundkenntnisse in Cisco IOS-Netzwerken und -Konzepten
- Vertrautheit mit den Grundlagen von Netzwerksicherheitskonzepten.

Lernziel

Sie machen sich mit der Implementierung der wichtigsten Sicherheitstechnologien vertraut und lernen bewährte Methoden mit Cisco-Sicherheitslösungen kennen.

Zielgruppe

- Security-, Network-Engineer und Network Administrator
- Systems Engineer.

Kursinhalt

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

- Describing Information Security Concepts*
  - Information Security Overview
  - Managing Risk
  - Vulnerability Assessment
  - Understanding CVSS
- 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
- 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
- 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

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

- 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
- 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
- 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

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

- 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
- 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
- Deploying Cisco Umbrella*
  - Cisco Umbrella Architecture
  - Deploying Cisco Umbrella
  - Cisco Umbrella Roaming Client
  - Managing Cisco Umbrella
  - Cisco Umbrella Investigate Overview
- Explaining VPN Technologies and Cryptography
  - VPN Definition
  - VPN Types
  - Secure Communication and Cryptographic Services
  - Keys in Cryptography
  - Public Key Infrastructure
- 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
- Deploying Cisco IOS VTI-Based Point-to-Point
  - Cisco IOS VTIs
  - Static VTI Point-to-Point IPsec IKEv2 VPN Configuration
- 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

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

- Introducing Cisco Secure Remote Access VPN Solutions
  - Remote Access VPN Components
  - Remote Access VPN Technologies
  - SSL Overview
- 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
- 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
- Describing 802.1X Authentication
  - 802.1X and EAP
  - EAP Methods
  - Role of RADIUS in 802.1X Communications
  - RADIUS Change of Authorization
- 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
- 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
- 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
- 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

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

- Deploying Control Plane Security Controls*
  - Infrastructure ACLs
  - Control Plane Policing
  - Control Plane Protection
  - Routing Protocol Security
- 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
- Deploying Layer 3 Data Plane Security Controls*
  - Infrastructure Antispoofing ACLs
  - Unicast Reverse Path Forwarding
  - IP Source Guard.

Laborübungen

- Configure Network Settings And NAT On Cisco ASA
- Configure Cisco ASA Access Control Policies
- Configure Cisco Firepower NGFW NAT
- Configure Cisco Firepower NGFW Access Control Policy
- Configure Cisco Firepower NGFW Discovery and IPS Policy
- Configure Cisco NGFW Malware and File Policy
- Configure Listener, HAT, and RAT on Cisco ESA
- Configure Mail Policies
- Configure Proxy Services, Authentication, and HTTPS Decryption
- Enforce Acceptable Use Control and Malware Protection
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore DNS Ransomware Protection by Cisco Umbrella
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
- Configure Remote Access VPN on the Cisco Firepower NGFW
- Explore Cisco AMP for Endpoints
- Perform Endpoint Analysis Using AMP for Endpoints Console
- Explore File Ransomware Protection by Cisco AMP for Endpoints Console
- Explore Cisco Stealthwatch Enterprise v6.9.3
- Explore CTA in Stealthwatch Enterprise v7.0
- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors.

Zertifizierung

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

Implementing and Operating Cisco Security Core Technologies v1.0 (SCOR 300-701) ist eine 120-minütige Prüfung für die Zertifizierungen CCNP Security, CCIE Security und Cisco Certified Specialist - Security Core. Diese Prüfung testet das Wissen eines Kandidaten über die Implementierung und den Betrieb von zentralen Sicherheitstechnologien, einschliesslich Netzwerksicherheit, Cloud-Sicherheit, Inhaltssicherheit, Endpunktschutz und -erkennung, sicherem Netzwerkzugriff, Sichtbarkeit und Durchsetzung. Der Kurs Implementierung und Betrieb von Cisco Security Core Technologies hilft den Kandidaten, sich auf diese Prüfung vorzubereiten.

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100