

In diesem Kurs erlernen Sie die Fähigkeiten und Technologien, um grundlegende Cisco-Sicherheitslösungen zu implementieren und einen erweiterten Bedrohungsschutz gegen Cybersicherheitsangriffe zu bieten. Sie lernen Sicherheit für Netzwerke, Cloud und Inhalte, Endpunktschutz, sicheren Netzwerkzugriff, Sichtbarkeit und Durchsetzungen kennen. Sie erhalten umfangreiche praktische Erfahrungen mit der Bereitstellung von Cisco Firepower® Next-Generation Firewall und Cisco Adaptive Security Appliance (ASA)-Firewall. Sie erhalten Einführungsübungen zu Cisco Stealthwatch® Enterprise und Cisco Stealthwatch Cloud-Bedrohungserkennungsfunktionen.

Kursinhalt

- Describing Information Security Concepts*
- Describing Common TCP/IP Attacks*
- Describing Common Network Application Attacks*
- Describing Common Endpoint Attacks*
- Describing Network Security Technologies
- Deploying Cisco ASA Firewall
- Deploying Cisco Firepower Next-Generation Firewall
- Deploying Email Content Security
- Deploying Web Content Security
- Deploying Cisco Umbrella*
- Explaining VPN Technologies and Cryptography
- Introducing Cisco Secure Site-to-Site VPN Solutions
- Deploying Cisco IOS VTI-Based Point-to-Point
- Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW
- Introducing Cisco Secure Remote Access VPN Solutions
- Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW
- Explaining Cisco Secure Network Access Solutions*
- Describing 802.1X Authentication*
- Configuring 802.1X Authentication*
- Describing Endpoint Security Technologies*
- Deploying Cisco AMP for Endpoints*
- Introducing Network Infrastructure Protection*
- Deploying Control Plane Security Controls*
- Deploying Layer 2 Data Plane Security Controls*
- Deploying Layer 3 Data Plane Security Controls*

* This section is self-study material that can be done at your own pace if you are taking the instructor-led version of this course.

E-Book Sie erhalten die englischen Original-Unterlagen als Cisco E-Book. Bei der Cisco Digital Learning Version sind die Inhalte der Kursunterlage stattdessen in die Lernoberfläche integriert.

Zielgruppe

- Sicherheitstechniker
- Netzwerktechniker
- Netzwerkdesigner
- Netzwerkadministratoren
- Systemtechniker
- Netzwerkmanager
- Projektmanager

Voraussetzungen

- Vertrautheit mit Ethernet- und TCP / IP-Netzwerken
- Grundkenntnisse des Windows-Betriebssystems

Bearbeitungszeit

ca. 30 Stunden

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/SCOR

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Cisco Digital Learning & Cisco U.

Die multimodalen Schulungen der Cisco Digital Learning Library beinhalten referenzgeführte HD-Videos mit hinterlegtem durchsuchbarem Text und Untertiteln, Übungen, Labs und erklärenden Text sowie Grafiken. Das Angebot stellen wir Ihnen über unser Lernportal myExperTeach zur Verfügung. Der Zugriff auf die Kurse steht ab der Freischaltung für einen Zeitraum von sechs Monaten zur Verfügung. Bei Paketen (Cisco U.) beträgt dieser Zeitraum zwölf Monate.

Cisco Digital Learning & Cisco U. Preise zzgl. MwSt.

6 Monate Freischaltung € 500,-

Training Preise zzgl. MwSt.

Termin/Kursort	Termin	Termin	Preis
Termine in Deutschland	5 Tage		€ 3.595,-
Termine in der Schweiz	5 Tage		€ 4.700,-
Online Training	5 Tage		€ 3.595,-
Kurs Sprache Deutsch 			
03.06.-07.06.24	 Düsseldorf	21.10.-25.10.24	Berlin
03.06.-07.06.24	 Online	21.10.-25.10.24	 Hamburg
24.06.-28.06.24	Zürich	21.10.-25.10.24	 Online
08.07.-12.07.24	 Düsseldorf	04.11.-08.11.24	Zürich
08.07.-12.07.24	 Online	25.11.-29.11.24	 München
12.08.-16.08.24	 Düsseldorf	25.11.-29.11.24	 Online
12.08.-16.08.24	 Online		

Stand 28.04.2024



Inhaltsverzeichnis

SCOR – Implementing and Operating Cisco Security Core Technologies

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

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

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

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

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

* This section is self-study material that can be done at your own pace if you are taking the instructor-led version of this course.

