

Cisco - Implementing and Operating Cisco Security Core Technologies (SCOR)

In diesem Kurs erwerben Sie die Fähigkeiten und den Einsatz von Technologien, die Sie benötigen, um die Kern-Sicherheitslösungen von Cisco zu implementieren, um fortschrittlichen Schutz vor Cybersecurity-Angriffen zu bieten. Sie lernen Sicherheit für Netzwerke, Cloud und Content, Endpunktschutz, sicheren Netzwerkzugang, Sichtbarkeit und Enforcement zu Implementieren. Sie erhalten umfangreiche praktische Erfahrungen bei der Implementierung der Cisco Firepower Next-Generation Firewall und der Cisco ASA Firewall, der Konfiguration von Zugriffskontrollrichtlinien, Mail-Richtlinien und 802.1X-Authentifizierung und vielem mehr. Außerdem erhalten Sie eine Einführung in die Funktionen zur Bedrohungserkennung 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, die zu den neuen Zertifizierungen CCNP Security, CCIE Security und Cisco Certified Specialist - Security Core führt.

Angesprochener Teilnehmerkreis:

- Sicherheitsingenieur
- Netzwerktechniker
- Netzwerk-Designer
- Netzwerkadministrator
- Systemingenieur
- Beratender Systemingenieur
- Architekt für technische Lösungen
- Cisco Integratoren/Partner
- Netzwerk-Manager
- Cisco Integratoren und Partner

Hinweis:

Kursprache ist Deutsch, die Unterlagen sind in englischer Sprache (teilweise in digitaler Form). Dieses Seminar führen wir in Kooperation mit der Fast Lane GmbH durch.

Seminar- bzw. Schulungsinhalte

- Beschreiben von Informationssicherheitskonzepten*
 - Überblick über die Informationssicherheit
 - Risikomanagement
 - Bewertung der Verwundbarkeit
 - CVSS verstehen
- Beschreibung gängiger TCP/IP-Angriffe*
 - Legacy TCP/IP-Sicherheitslücken
 - IP-Schwachstellen
 - ICMP-Schwachstellen
 - TCP-Sicherheitslücken
 - UDP-Sicherheitslücken

- Angriffsfläche und Angriffsvektoren
- Aufklärungsangriffe
- Zugriffsangriffe
- Man-In-The-Middle-Angriffe
- Denial-of-Service- und Distributed-Denial-of-Service-Angriffe
- Reflexions- und Verstärkungsangriffe
- Spoofing-Angriffe
- DHCP-Angriffe

- Beschreibung gängiger Angriffe auf Netzwerkanwendungen*
 - Passwort-Angriffe
 - DNS-basierte Angriffe
 - DNS-Tunneling
 - Web-basierte Angriffe
 - HTTP 302 Dämpfung
 - Befehlsinjektionen
 - SQL-Injektionen
 - Cross-Site Scripting und Request Forgery
 - E-Mail-basierte Angriffe

- Beschreibung gängiger Endpunkt-Angriffe*
 - Pufferüberlauf
 - Malware
 - Aufklärungsangriff
 - Zugriff und Kontrolle erlangen
 - Zugang über Social Engineering erlangen
 - Zugriff über webbasierte Angriffe erlangen
 - Exploit-Kits und Rootkits
 - Privileg-Eskalation
 - Nachnutzungsphase
 - Angler Exploit Kit

- Beschreiben von Netzwerksicherheitstechnologien
 - Defense-in-Depth-Strategie
 - Verteidigung über das gesamte Angriffskontinuum
 - Netzwerksegmentierung und Virtualisierung im Überblick
 - Überblick über die Stateful Firewall
 - Security Intelligence Übersicht
 - Standardisierung von Bedrohungsinformationen
 - Überblick über den netzwerkbasierten Schutz vor Malware
 - IPS Übersicht
 - Übersicht über die Firewall der nächsten Generation
 - Übersicht über die Sicherheit von E-Mail-Inhalten
 - Web Content Security Übersicht
 - Threat-Analytic-Systeme im Überblick
 - DNS-Sicherheitsübersicht
 - Überblick über Authentifizierung, Autorisierung und Abrechnung
 - Überblick über Identitäts- und Zugriffsmanagement

- Überblick über die Virtual Private Network-Technologie
- Übersicht der Formfaktoren von Netzwerksicherheitsgeräten

- Einsatz der Cisco ASA Firewall
 - Cisco ASA-Implementierungstypen
 - Sicherheitsstufen der Cisco ASA-Schnittstelle
 - Cisco ASA-Objekte und Objektgruppen
 - Netzwerk-Adressübersetzung
 - Cisco ASA Schnittstellen-ACLs
 - Cisco ASA Globale ACLs
 - Cisco ASA Advanced Access Policies
 - Cisco ASA Hochverfügbarkeit Übersicht

- Einsatz der Cisco Firepower Next-Generation Firewall
 - Cisco Firepower NGFW-Einsätze
 - Cisco Firepower NGFW Paketverarbeitung und -richtlinien
 - Cisco Firepower NGFW-Objekte
 - Cisco Firepower NGFW NAT
 - Cisco Firepower NGFW Vorfilter-Richtlinien
 - Cisco Firepower NGFW Zugriffskontrollrichtlinien
 - Cisco Firepower NGFW Security Intelligence
 - Cisco Firepower NGFW Erkennungsrichtlinien
 - Cisco Firepower NGFW IPS-Richtlinien
 - Cisco Firepower NGFW Malware- und Dateirichtlinien

- Einsatz von E-Mail-Inhaltssicherheit
 - Cisco Email Content Security Übersicht
 - SMTP-Übersicht
 - E-Mail-Pipeline Übersicht
 - Öffentliche und private Hörer
 - Host Access Table Übersicht
 - Empfängerzugriffstabelle Übersicht
 - Mail-Richtlinien Übersicht
 - Schutz vor Spam und Graymail
 - Antiviren- und Antimalware-Schutz
 - Filter für Ausbrüche
 - Content Filters
 - Schutz vor Datenverlust
 - E-Mail-Verschlüsselung

- Einsatz von Web Content Security
 - Cisco WSA Übersicht
 - Bereitstellungsoptionen
 - Netzwerkbenutzer-Authentifizierung
 - Entschlüsselung des HTTPS-Verkehrs
 - Zugriffsrichtlinien und Identifikationsprofile
 - Einstellungen für die Steuerung der akzeptablen Nutzung
 - Anti-Malware-Schutz

- Einsatz von Cisco Umbrella*
 - Cisco Umbrella-Architektur
 - Bereitstellen von Cisco Umbrella
 - Cisco Umbrella Roaming Client
 - Cisco Umbrella verwalten
 - Cisco Umbrella Investigate Übersicht
- Erklärungen zu VPN-Technologien und Kryptographie
 - VPN Definition
 - VPN-Typen
 - Sichere Kommunikation und kryptografische Dienste
 - Schlüssel in der Kryptographie
 - Infrastruktur für öffentliche Schlüssel
- Einführung in die sicheren Site-to-Site-VPN-Lösungen von Cisco
 - Standort-zu-Standort-VPN-Topologien
 - IPsec VPN Übersicht
 - IPsec Statische Krypto-Maps
 - IPsec Statische virtuelle Tunnelschnittstelle
 - Dynamisches Mehrpunkt-VPN
 - Cisco IOS FlexVPN
- Einsatz von Cisco IOS VTI-basiertem Punkt-zu-Punkt
 - Cisco IOS VTIs
 - Statische VTI Punkt-zu-Punkt IPsec IKEv2 VPN-Konfiguration
- Bereitstellen von Punkt-zu-Punkt-IPsec-VPNs auf der Cisco ASA und Cisco Firepower NGFW
 - Punkt-zu-Punkt-VPNs auf der Cisco ASA und Cisco Firepower NGFW
 - Cisco ASA Punkt-zu-Punkt-VPN-Konfiguration
 - Cisco Firepower NGFW Punkt-zu-Punkt-VPN-Konfiguration
- Einführung in die Cisco Secure Remote Access VPN-Lösungen
 - Fernzugriff VPN-Komponenten
 - Fernzugriff VPN-Technologien
 - SSL-Übersicht
- Bereitstellen von Remote Access SSL-VPNs auf der Cisco ASA und Cisco Firepower NGFW
 - Konzepte für die Fernzugriffskonfiguration
 - Verbindungsprofile
 - Gruppenrichtlinien
 - Cisco ASA Remote Access VPN-Konfiguration
 - Cisco Firepower NGFW Fernzugriff VPN-Konfiguration
- Erklärungen zu Cisco Secure Network Access-Lösungen
 - Cisco Secure Network Access
 - Cisco Secure Network Access Komponenten
 - AAA-Rolle in der Cisco Secure Network Access-Lösung
 - Cisco Identity Services Engine

- Cisco TrustSec
- Beschreiben der 802.1X-Authentifizierung
 - 802.1X und EAP
 - EAP-Methoden
 - Rolle von RADIUS in der 802.1X-Kommunikation
 - RADIUS Änderung der Berechtigung
- Konfigurieren der 802.1X-Authentifizierung
 - Cisco Catalyst Switch 802.1X Konfiguration
 - Cisco WLC 802.1X Konfiguration
 - Cisco ISE 802.1X Konfiguration
 - Supplicant 802.1x Konfiguration
 - Cisco Zentrale Web-Authentifizierung
- Beschreibung der Endpunktsicherheitstechnologien*
 - Host-basierte Personal Firewall
 - Host-basiertes Anti-Virus
 - Host-basiertes Intrusion Prevention System
 - Anwendungs-Whitelists und -Blacklists
 - Host-basierter Schutz vor Malware
 - Sandboxing Übersicht
 - Prüfung der Dateiintegrität
- Bereitstellen von Cisco AMP für Endpunkte*
 - Cisco AMP für Endpunkte Architektur
 - Cisco AMP for Endpoints Engines
 - Retrospektive Sicherheit mit Cisco AMP
 - Cisco AMP-Gerät und Datei-Trajektorie
 - Cisco AMP für Endpunkte verwalten
- Einführung in den Schutz der Netzwerkinfrastruktur*
 - Identifizieren von Netzwerkgeräteebenen
 - Sicherheitskontrollen der Steuerungsebene
 - Sicherheitskontrollen der Managementebene
 - Netzwerk-Telemetry
 - Sicherheitskontrollen der Layer-2-Datenebene
 - Sicherheitskontrollen der Layer-3-Datenebene
- Einsatz von Sicherheitskontrollen der Steuerungsebene*
 - Infrastruktur ACLs
 - Control Plane Policing
 - Schutz der Steuerungsebene
 - Routing-Protokoll Sicherheit
- Einsatz von Layer 2 Data Plane Security Controls*
 - Übersicht über die Sicherheitskontrollen der Layer-2-Datenebene
 - VLAN-basierte Angriffe abwehren

- STP-Angriffe Entschärfung
 - Hafensicherheit
 - Private VLANs
 - DHCP Snooping
 - ARP-Prüfung
 - Sturmsteuerung
 - MACsec-Verschlüsselung
- Einsatz von Layer 3 Data Plane Security Controls*
 - Infrastruktur Antispoofing ACLs
 - Unicast Umgekehrte Pfadweiterleitung
 - IP Source Guard
 - * Dieser Abschnitt ist Material zum Selbststudium, das Sie in Ihrem eigenen Tempo bearbeiten können, wenn Sie die von einem Kursleiter geleitete Version dieses Kurses besuchen.

Seminar- bzw. Schulungsvoraussetzungen

Um von diesem Kurs in vollem Umfang zu profitieren, sollten Sie über die folgenden Kenntnisse und Fähigkeiten verfügen:

- Fertigkeiten und Kenntnisse, die denen des Kurses Implementing and Administering Cisco Solutions (CCNA) v1.0 entsprechen
- Vertrautheit mit Ethernet und TCP/IP-Netzwerken
- Kenntnisse im Umgang mit dem Betriebssystem Windows
- Kenntnisse über Cisco IOS-Netzwerke und Konzepte
- Vertrautheit mit den Grundlagen von Netzwerksicherheitskonzepten

Seminarart

Dieses Seminar können Sie als **Präsenzseminar** oder als **Live-Online-Training** (virtuelles Präsenzseminar) buchen.

Dauer

5 Tage von 10:00 bis 17:30 Uhr

Preise

Die Teilnahmegebühr beträgt 3.595,00 € (4.278,05 € inkl. 19% MwSt.)

Im Preis enthalten sind Kursmaterial, Pausenverpflegung, Getränke und Schulungszertifikat.

Anmeldung

Bitte **online** anmelden oder per **Fax**.

Termine

Die aktuellen Termine und Standorte für Cisco - Implementing and Operating Cisco Security Core Technologies (SCOR) finden Sie [online](#).

Weitere Seminare

Alle Seminare finden Sie in unserer [Seminarübersicht](#).

Gerne unterbreiten wir Ihnen auch ein individuelles Angebot entsprechend Ihrer Wünsche und Vorstellungen. Senden Sie hierfür Ihre Anfrage einfach an training@pc-college.de.

Erstellt am 29.03.2024

Viele Partner für ein Ziel: Beste Leistung und Rundum-Service

Live-Online-Training

Berlin
Bremen
Dortmund
Dresden
Düsseldorf
Erfurt
Essen
Frankfurt
Freiburg
Hamburg
Hannover
Jena
Karlsruhe
Kassel
Koblenz
Köln
Krefeld
Leipzig
Mannheim
München
Münster
Nürnberg
Paderborn
Regensburg
Saarbrücken
Siegen
Stuttgart
A-Wien
CH-Basel
CH-Bern
CH-Zürich



PC-COLLEGE Zentrale Berlin

Stresemannstraße 78 (Nähe Potsdamer Platz) | D-10963 Berlin
Telefon: 0800 5777 333 / +49 (0)30 235 0000 | Fax: +49 30 2142988 | E-Mail: training@pc-college.de
Ansprechpartner*in: Stefanie Wendt und Kollegen*innen

Alle Informationen und Aktionsangebote finden Sie unter www.pc-college.de