Implementing and Operating Cisco Security Core Technologies (SCOR)

ID SCOR **Preis** 3.595,– € (exkl. MwSt.) **Dauer** 5 Tage

Dieser Text wurde automatisiert übersetzt. Um den englischen Originaltext anzuzeigen, klicken Sie bitte hier.

Kursüberblick

Der Kurs Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 unterstützt Sie bei der Vorbereitung auf die Cisco® CCNP® Security und CCIE® Security Zertifizierungen und auf Senior-Level Security Rollen. In diesem Kurs werden Sie die Fähigkeiten und Technologien beherrschen, 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. 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. Sie erhalten 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.

Zielgruppe

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

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Network Professional Security (CCNP SECURITY)

Voraussetzungen

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

Kursziele

Nach dem Besuch dieses Kurses sollten Sie in der Lage sein:

- Konzepte und Strategien der Informationssicherheit im Netzwerk beschreiben
- Beschreiben Sie gängige TCP/IP-, Netzwerkanwendungs- und Endpunkt-Angriffe
- Beschreiben, wie verschiedene Netzwerksicherheitstechnologien zum Schutz vor Angriffen zusammenarbeiten
- Zugriffskontrolle auf Cisco ASA-Appliance und Cisco Firepower Next-Generation Firewall implementieren
- Beschreiben und Implementieren grundlegender Sicherheitsmerkmale und -funktionen für E-Mail-Inhalte, die von der Cisco Email Security Appliance bereitgestellt werden
- Beschreiben und Implementieren der von der Cisco Web Security Appliance bereitgestellten Features und Funktionen für die Sicherheit von Webinhalten
- Beschreiben Sie die Sicherheitsfunktionen von Cisco Umbrella, die Bereitstellungsmodelle, die

Richtlinienverwaltung und die Untersuchungskonsole
- VPNs einführen und Kryptographie-Lösungen und -Algorithmen beschreiben
- Beschreiben Sie Cisco-Lösungen für sichere Site-to-Site-Konnektivität und erklären Sie, wie Sie Cisco IOS VTI-basierte Punkt-zu-Punkt-IPsec-VPNs und Punkt-zu-Punkt-IPsec-VPNs auf der Cisco ASA und der Cisco FirePower NGFW implementieren
- Beschreiben und Bereitstellen von Cisco Secure Remote Access Connectivity-Lösungen und Beschreiben der Konfiguration von 802.1X und EAP-Authentifizierung
- Vermittlung eines grundlegenden Verständnisses der Endpunktsicherheit und Beschreibung der Architektur und der grundlegenden Funktionen von AMP for Endpoints
- Untersuchen Sie verschiedene Verteidigungsmaßnahmen auf Cisco-Geräten, die die Kontroll- und Verwaltungsebene schützen
- Konfigurieren und verifizieren Sie die Cisco IOS Software Layer 2 und Layer 3 Data Plane Controls
- Beschreiben Sie die Lösungen Cisco Stealthwatch Enterprise und Stealthwatch Cloud
- Beschreiben Sie die Grundlagen des Cloud Computing und gängige Cloud-Angriffe und wie man eine Cloud-Umgebung absichert.

Dieser Kurs wird Ihnen helfen:

- Sammeln Sie praktische Erfahrungen bei der Implementierung zentraler Sicherheitstechnologien und lernen Sie Best Practices mit Cisco Sicherheitslösungen kennen
- Bereiten Sie sich auf die Prüfung Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) vor
- Qualifizieren Sie sich für Sicherheitsjobs auf Fach- und Expertenebene

Dieser Kurs unterstützt Sie bei der Vorbereitung auf die Prüfung Implementing and Operating Cisco Security Core Technologies (350-701 SCOR). Diese Prüfung testet das Wissen eines Kandidaten über die Implementierung und den Betrieb von Kernsicherheitstechnologien.

Kursinhalt

- Beschreiben von Informationssicherheitskonzepten*
- Beschreibung gängiger TCP/IP-Angriffe*
- Beschreibung gängiger Angriffe auf Netzwerkanwendungen*
- Beschreibung gängiger Endpunkt-Angriffe*
- Beschreiben von Netzwerksicherheitstechnologien
- Einsatz der Cisco ASA Firewall
- Einsatz der Cisco Firepower Next-Generation Firewall
- Einsatz von E-Mail-Inhaltssicherheit
- Einsatz von Web Content Security
- Einsatz von Cisco Umbrella*
- Erklärungen zu VPN-Technologien und Kryptographie
- Einführung in die sicheren Site-to-Site-VPN-Lösungen von Cisco
- Einsatz von Cisco IOS VTI-basiertem Punkt-zu-Punkt
- Bereitstellen von Punkt-zu-Punkt-IPsec-VPNs auf der Cisco ASA und Cisco Firepower NGFW
- Einführung in die Cisco Secure Remote Access VPN-Lösungen
- Bereitstellen von Remote Access SSL-VPNs auf der Cisco ASA und Cisco Firepower NGFW
- Erklärungen zu Cisco Secure Network Access-Lösungen
- Beschreiben der 802.1X-Authentifizierung
- Konfigurieren der 802.1X-Authentifizierung
- Beschreibung der Endpunktsicherheitstechnologien*
- Bereitstellen von Cisco AMP für Endpunkte*
- Einführung in den Schutz der Netzwerkinfrastruktur*
- Einsatz von Sicherheitskontrollen der Steuerungsebene*
- Einsatz von Layer 2 Data Plane Security Controls*
- Einsatz von Layer 3 Data Plane Security Controls*
- Einsatz von Sicherheitskontrollen der Managementebene*
- Einsatz von Verkehrstelemetrie-Methoden*
- Einsatz von Cisco Stealthwatch Enterprise*
- Beschreibung der Cloud und gängiger Cloud-Angriffe*
- Absicherung der Cloud*
- Bereitstellen von Cisco Stealthwatch Cloud*
- Beschreiben von Software-Defined Networking (SDN*)

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.

Detaillierter Kursinhalt

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-Telemetrie
- 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.

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch