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

Das Training **Implementing and Operating Cisco Security Core Technologies (SCOR)** vermittelt Ihnen die Fähigkeiten und Technologien, die Sie für die Implementierung der wichtigsten Cisco Sicherheitslösungen benötigen. Mit diesem Training sind Sie in der Lage, fortschrittlichen Schutz vor Cybersecurity-Angriffen zu bieten und sich auf leitende Sicherheitsfunktionen vorzubereiten.

Dieses Training bereitet Sie auf die Prüfung 350-701 SCOR v1.0 vor. Bei Bestehen erhalten Sie die Cisco Certified Specialist - Security Core Zertifizierung und erfüllen die Kernprüfungsanforderungen für die Cisco Certified Network Professional (CCNP) Security und Cisco Certified Internetwork Expert (CCIE) Security Zertifizierungen. Mit diesem Training erhalten Sie außerdem 64 Continuing Education (CE) Credits für die Rezertifizierung.

Wie Sie davon profitieren

Diese Schulung wird Ihnen helfen:

- Sammeln Sie praktische Erfahrungen bei der Implementierung zentraler Sicherheitstechnologien und lernen Sie Best Practices mit Cisco Sicherheitslösungen kennen.
- Qualifizieren Sie sich für Sicherheitsberufe auf Fach- und Expertenebene
- Vorbereitung auf die Prüfung 350-701 SCOR v1.0
- Erwerben Sie 64 CE-Punkte für die Rezertifizierung

Was Sie bei der Prüfung erwartet

Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) v1.0 ist eine 120-minütige Prüfung, die mit der Cisco Certified Specialist - Security Core Zertifizierung verbunden ist und die Kernprüfungsanforderungen für die CCNP Security und CCIE Security Zertifizierungen erfüllt.

Diese Prüfung prüft Ihr Wissen über die Implementierung und den Betrieb der wichtigsten Sicherheitstechnologien, einschließlich:

- Sicherheit im Netz
- Sicherheit in der Cloud
- Sicherheit des Inhalts
- Endpunktschutz und -erkennung
- Sicherer Netzzugang
- Sichtbarkeit und Durchsetzung

Zielgruppe

- Sicherheitsingenieure
- Netzwerk-Ingenieure
- Netzwerk-Designer
- Netzwerk-Administratoren
- Systemingenieure
- Beratende Systemingenieure
- Architekten für technische Lösungen
- Cisco Integratoren und Partner
- Netzwerk-Manager
- Program Managers
- Projektleiter

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Network Professional Security (CCNP SECURITY)

Voraussetzungen

Für diese Schulung gibt es keine formalen Voraussetzungen. Es wird jedoch empfohlen, dass Sie vor der Teilnahme an dieser Schulung folgende Kenntnisse und Fähigkeiten besitzen:

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

- Kenntnisse von Cisco IOS-Netzwerken und Konzepten
- Vertrautheit mit den Grundlagen des Netzwerksicherheitskonzepts

s Diese Fähigkeiten sind in den folgenden Cisco-Lernangeboten zu finden:

- Implementing and Administering Cisco Solutions (CCNA) v2.1

Kursziele

Nach der Teilnahme an diesem Kurs sollten Sie in der Lage sein:

- Konzepte und Strategien der Informationssicherheit innerhalb des Netzes zu beschreiben
- Beschreibung von Sicherheitslücken im Übertragungsprotokoll/Internetprotokoll (TCP/IP) und wie diese für Angriffe auf Netzwerke und Hosts genutzt werden können
- Beschreiben Sie netzwerkanwendungsbasierte Angriffe
- Beschreiben, wie verschiedene Netzsicherheitstechnologien zusammenarbeiten, um Angriffe abzuwehren
- Implementierung der Zugriffskontrolle auf der Cisco Secure Firewall Adaptive Security Appliance (ASA)
- Bereitstellung der Grundkonfigurationen von Cisco Secure Firewall Threat Defense
- Einsatz von Cisco Secure Firewall Threat Defense IPS, Malware- und Fire-Richtlinien
- Bereitstellung der Grundkonfigurationen von Cisco Secure Email Gateway
- Bereitstellung von Cisco Secure Email Gateway-Richtlinienkonfigurationen
- Beschreiben und Implementieren grundlegender Sicherheitsmerkmale und -funktionen für Webinhalte, die von Cisco Secure Web Appliance bereitgestellt werden
- Beschreiben Sie verschiedene Angriffstechniken gegen die Endpunkte
- Beschreiben Sie die Sicherheitsfunktionen von Cisco Umbrella®, die Bereitstellungsmodelle, die Richtlinienverwaltung und die Investigate-Konsole.
- Grundlegendes Verständnis der Endpunktsicherheit und Vertrautheit mit gängigen Endpunktsicherheitstechnologien
- Beschreiben Sie die Architektur und die grundlegenden Funktionen von Cisco Secure Endpoint
- Beschreiben Sie die Cisco Secure Network Access-Lösungen
- Beschreibung von 802.1X und EAP-Authentifizierung (Extensible Authentication Protocol)
- Konfigurieren Sie Geräte für 802.1X-Operationen
- Einführung in VPNs und Beschreibung von Kryptographielösungen und -algorithmen
- Beschreiben Sie die sicheren Site-to-Site-Konnektivitätslösungen von Cisco
- Bereitstellung von Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-basierten Punkt-zu-Punkt IPsec VPNs
- Konfigurieren von Punkt-zu-Punkt-IPsec-VPNs auf Cisco Secure Firewall ASA und Cisco Secure Firewall Threat Defense
- Beschreiben Sie die Cisco-Lösungen für den sicheren Fernzugriff
- Bereitstellung von sicheren Cisco-Lösungen für den Fernzugriff
- einen Überblick über die Kontrollen zum Schutz der Netzinfrastruktur zu geben
- Untersuchung verschiedener Schutzmaßnahmen auf Cisco-Geräten, die die Steuerungsebene schützen
- Konfiguration und Überprüfung von Cisco IOS Software Layer 2 Data Plane Controls
- Konfiguration und Überprüfung der Cisco IOS Software und der Cisco ASA Layer 3 Data Plane Controls
- Untersuchen Sie verschiedene Schutzmaßnahmen auf Cisco-Geräten, die die Verwaltungsebene schützen.
- Beschreiben Sie die grundlegenden Formen der Telemetrie, die für Netzinfrastruktur- und Sicherheitsgeräte empfohlen werden.
- Beschreiben Sie die Bereitstellung von Cisco Secure Network Analytics
- Beschreibung der Grundlagen des Cloud Computing und gängiger Cloud-Angriffe
- Beschreiben Sie, wie man eine Cloud-Umgebung sichert
- Beschreiben Sie den Einsatz von Cisco Secure Cloud Analytics
- Beschreibung der Grundlagen von softwaredefinierten Netzwerken und Netzwerkprogrammierbarkeit

Detaillierter Kursinhalt

- Netzwerksicherheitstechnologien
- Cisco Secure Firewall ASA-Bereitstellung
- Grundlagen der Cisco Secure Firewall-Bedrohungsabwehr
- Cisco Secure Firewall Bedrohungsabwehr IPS, Malware und Dateirichtlinien
- Grundlagen des Cisco Secure Email Gateway
- Konfiguration der Cisco Secure Email Policy
- Einsatz der Cisco Secure Web Appliance
- VPN-Technologien und Kryptographie-Konzepte
- Sichere Site-to-Site-VPN-Lösungen von Cisco
- Cisco IOS VTI-Based Point-to-Point IPsec VPNs
- Punkt-zu-Punkt-IPsec-VPNs auf Cisco Secure Firewall ASA und Cisco Secure Firewall Threat Defense
- Cisco Secure Remote-Access VPN-Lösungen
- Remote-Access-SSL-VPNs auf der Cisco Secure Firewall

ASA und Cisco Secure Firewall Threat Defense

- Beschreibung von Informationssicherheitskonzepten
- Beschreiben Sie gängige TCP/IP-Angriffe
- Beschreiben Sie gängige Angriffe auf Netzwerkanwendungen
- Häufige Endpunkt-Angriffe
- Cisco Umbrella Deployment
- Technologien zur Endpunktsicherheit
- Cisco Sicherer Endpunkt
- Sichere Netzwerkzugangslösungen von Cisco
- 802.1X-Authentifizierung
- Konfiguration der 802.1X-Authentifizierung
- Schutz der Netzinfrastruktur
- Sicherheitslösungen für die Steuerungsebene
- Sicherheitskontrollen der Schicht 2 der Datenebene
- Sicherheitskontrollen der Schicht 3 der Datenebene
- Sicherheitskontrollen auf der Verwaltungsebene
- Methoden der Verkehrstelemetrie
- Cisco Secure Network Analytics-Bereitstellung
- Cloud Computing und Cloud-Sicherheit
- Cloud-Sicherheit
- Cisco Secure Cloud Analytics-Bereitstellung
- Software-definierte Netzwerke

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