Implementing and Operating Cisco Security Core Technologies (SCOR)

ID SCOR **Preis** CHF 4'150.– (exkl. MwSt.) **Dauer** 5 Tage

Zielgruppe

- Sicherheitsingenieure
- Netzwerkingenieure
- Netzwerkplaner
- Netzwerkadministratoren
- Systemingenieure
- Beratende Systemingenieure
- Architekten für technische Lösungen
- Cisco-Integratoren und -Partner
- Netzwerkmanager
- Programmmanager
- Projektmanager

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Internetwork Expert (CCIE) Security (CCIE SECURITY)
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 über folgende Kenntnisse und Fähigkeiten verfügen:

- Kenntnisse im Bereich Ethernet- und TCP/IP-Netzwerke
- Praktische Kenntnisse des Windows-Betriebssystems
- Praktische Kenntnisse im Bereich Cisco IOS-Netzwerke und -Konzepte
- Kenntnisse der Grundlagen des Konzepts der Netzwerksicherheit

s Diese Kenntnisse werden im folgenden Cisco-Schulungsangebot vermittelt:

- Implementing and Administering Cisco Solutions (CCNA)

Kursziele

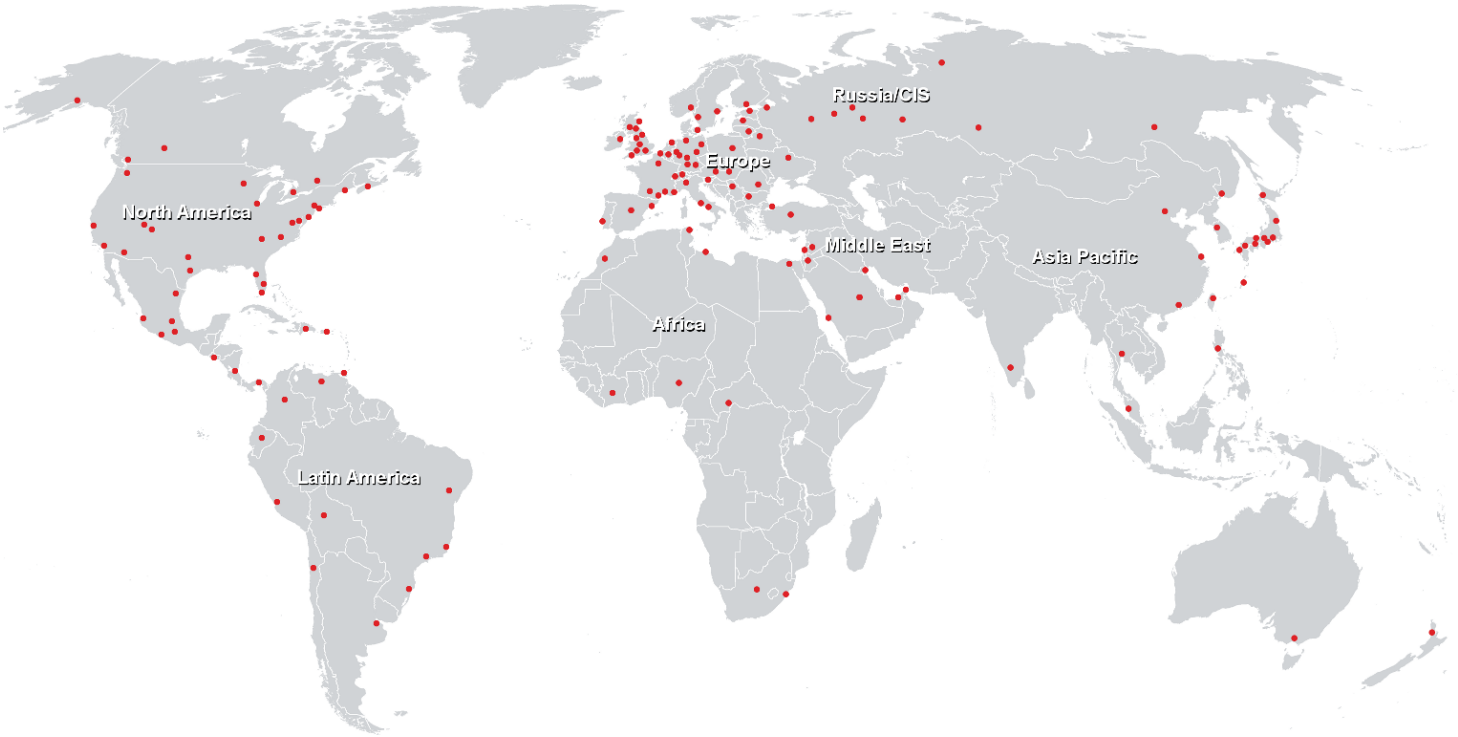
Nach Abschluss dieses Kurses sollten Sie in der Lage sein:

- Erläutern Sie, wie verschiedene Angreifer vorgehen, indem Sie deren Motive, gängige Angriffsvektoren, typische Muster bei Sicherheitsverletzungen und beim Missbrauch von Zugangsdaten sowie die Rolle des Lebenszyklus von Cyber-Bedrohungsinformationen beschreiben, der Unternehmen dabei hilft, diese sich ständig weiterentwickelnden Bedrohungen zu verstehen und zu verfolgen.
- Beschreiben Sie, wie strukturelle Schwachstellen in Software und Webanwendungen mithilfe von Konzepten wie Schwachstellenklassen, OWASP, CVE und CVSS identifiziert, klassifiziert und priorisiert werden, und erläutern Sie, wie KI-/LLM-Systeme diese Landschaft um neue Schwachstellenmuster erweitern.
- Erläutern Sie, warum Menschen und Identitäten nach wie vor einen der wichtigsten Angriffsvektoren darstellen, indem Sie den Lebenszyklus von Social-Engineering-Angriffen und dem Diebstahl von Zugangsdaten beschreiben und die wichtigsten konzeptionellen Verteidigungsebenen skizzieren, die Unternehmen einsetzen, um identitätsbezogene Risiken zu verringern, jedoch nicht vollständig zu beseitigen.
- Beschreiben Sie die wichtigsten kryptografischen Bausteine – Hash-Funktionen, symmetrische und asymmetrische Verschlüsselung, Schlüsselaustausch, digitale Signaturen, PKI und verschlüsselte Transportprotokolle – und erläutern Sie die spezifischen Sicherheitsgarantien und Vertrauensannahmen, die jeder dieser Bausteine in ein Unternehmensdesign einbringt.
- Erläutern Sie, wie Zero Trust, mehrschichtige Verteidigung und das Cisco SAFE Blueprint-Framework gemeinsam Erkenntnisse zu Bedrohungen, Schwachstellen, Identitäten und Kryptografie in eine kohärente Sicherheitsarchitektur umsetzen, die von möglichen Ausfällen ausgeht, den Schadensumfang begrenzt und als Leitfaden für den Einsatz von Technologien in der gesamten Umgebung dient.
- Erläutern Sie, warum das Layer-2-Zugangsnetz eine grundlegende Sicherheitsgrenze darstellt, indem Sie darlegen, wie Segmentierung, Topologie, Adressierung, Nachbarerkennung und Edge-Port-Kontrollen zusammenwirken, um zu verhindern, dass lokale Angriffe die Sicherheit höherer Schichten untergraben.
- Beschreiben Sie, wie Netzwerk-Infrastrukturgeräte gesichert werden können, indem ihre Angriffsfläche

verringert wird, die Verwaltungs- und Steuerungsebenen als privilegierte Autoritätskanäle geschützt werden und Architekturen für die Verwaltungsebene gewählt werden, die klare, vertretbare Vertrauensgrenzen schaffen.
- Erläutern Sie, wie AAA für die Infrastrukturverwaltung konzipiert und betrieben wird, indem Sie geeignete Protokolle auswählen, das AAA-Verhalten und das Fallback-Verhalten definieren sowie AAA-Ausfälle systematisch beheben, um einen sicheren administrativen Zugriff wiederherzustellen.
- Grundlegende Konfiguration der Cisco Secure Firewall Threat Defense durchführen
- Konfigurieren Sie die Zugriffskontrollrichtlinie zusammen mit der Richtlinie zum Schutz vor unbefugten Zugriffen sowie der Richtlinie für Dateien und Malware, um die vorgegebenen Sicherheitsanforderungen zu erfüllen.
- Konfigurieren Sie sichere Site-to-Site-VPN-Lösungen, um mithilfe von Cisco Secure Firewall Threat Defense eine Verbindung zwischen Remote-Standorten herzustellen
- Konfigurieren Sie VPN-Lösungen für den Fernzugriff auf der Cisco Secure Firewall Threat Defense, um Remote-Benutzern eine sichere Verbindung zum Unternehmensnetzwerk zu ermöglichen
- Bewertung von Cloud-Sicherheitsstrategien unter Verwendung der NIST 800-145-Modelle zur geteilten Verantwortung, von Sicherheits-Frameworks und CASB-Lösungen für Multi-Cloud-Umgebungen
- Beschreiben Sie Sicherheitsstrategien für Cloud-Workloads, die Prinzipien der Mikrosegmentierung, Cisco Secure Workload, Multicloud-Defense-Plattformen und eBPF-basierte Sicherheitsansätze umfassen.
- Beschreiben Sie die Prinzipien von DevSecOps und „Infrastructure as Code“ und interpretieren Sie Python-Skripte, um die API von Sicherheitsgeräten aufzurufen.
- Beschreiben Sie die SASE- und SSE-Architekturen sowie die Funktionen von Cisco Secure Access, die einen einheitlichen, cloudbasierten Schutz für private Anwendungen und das Internet in Remote- und Zweigstellenumgebungen bieten.
- Konfigurieren Sie Cloud-basierte Konnektivität, identitätsbasierte Authentifizierung und detaillierte Zugriffsrichtlinien, um Remote- und Zweigstellenbenutzern einen sicheren Zugriff auf private Anwendungen zu ermöglichen
- Konfigurieren Sie Verbindungsidentitäten und Sicherheitskontrollen, um Remote- und Zweigstellenbenutzern einen sicheren Zugriff auf das Internet und SaaS-Anwendungen zu ermöglichen
- Erläutern Sie, wie Identität, Gerätekontext und richtliniengesteuerte Zugriffskontrolle in Lösungen für sicheren Netzwerkzugang zusammenwirken, und beschreiben Sie, wie Cisco ISE einen differenzierten Zugriff durch AAA, Gastzugang, Profilerstellung und BYOD unterstützt.
- Konfigurieren Sie die Zugriffskontrolle für kabelgebundene und kabellose Netzwerke mit Cisco ISE, indem Sie 802.1X und MAB implementieren, die Authentifizierungs- und Autorisierungsrichtlinien von Cisco ISE anwenden, geeignete EAP- und Supplicant-Ansätze auswählen und RADIUS sowie CoA nutzen, um die Änderung des Zugriffsstatus durchzusetzen.
- Erläutern Sie, wie Cisco Duo die Zero-Trust-Prinzipien durch strenge Benutzerauthentifizierung, Gerätevertrauen, adaptive Zugriffsrichtlinien und Transparenz hinsichtlich Identitätsrisiken mithilfe von Cisco Identity Intelligence unterstützt.
- Erläutern Sie, wie Cisco Secure Email Threat Defense in Microsoft 365-basierten E-Mail-Umgebungen integriert und konfiguriert wird, um Transparenz bei Nachrichten, Bedrohungsanalysen und Abhilfemassnahmen gegen Phishing, Business E-Mail Compromise und die Übernahme von Konten zu gewährleisten.
- Erläutern Sie, wie Unternehmen durch Gerätemanagement, Transparenz der IT-Ressourcen, Compliance- und Sicherheitszustandsbewertung sowie Anwendungskontrolle Vertrauen in Endgeräte aufbauen, überprüfen und durchsetzen, um Sicherheitsrisiken an Endgeräten zu verringern.
- Erläutern Sie, wie moderne Endpunktsicherheit, wie beispielsweise „Cisco Secure Endpoint“ mit „Cisco Secure Malware Analytics“, Prävention, kontinuierliche Erkennung, Malware-Analyse und ereignisgesteuerte Untersuchungen mithilfe der Konzepte der Endpoint Protection Platform (EPP) und Endpoint Detection and Response (EDR) miteinander verbindet.
- Beschreiben Sie, wie Splunk Enterprise und Splunk Cloud als Datenanalyseplattformen für den Sicherheitsbetrieb fungieren, erläutern Sie, wie die Komponenten und Bereitstellungsmodelle der Splunk-Plattform eine skalierbare Datenverarbeitung und -analyse unterstützen, erstellen Sie Abfragen mithilfe der Splunk Processing Language, um die eingelesenen Daten zu durchsuchen und zu analysieren, erläutern Sie, wie Cisco-Sicherheitsprodukte in Splunk integriert sind, und beschreiben Sie, wie Splunk Enterprise die Plattform um SIEM-Funktionen erweitert.
- Erläutern Sie, wie Splunk SOAR den SOC-Betrieb durch Orchestrierung, Playbook-Automatisierung und fallgesteuerte Reaktion unterstützt, und beschreiben Sie, wie es mit Splunk Enterprise Security und Cisco XDR zusammenarbeitet, um Untersuchungs- und Reaktionsworkflows zu automatisieren.
- Erläutern Sie, wie XDR die Erkennung, Untersuchung und Reaktion auf Bedrohungen über mehrere Sicherheitsdomänen hinweg vereint, und beschreiben Sie, wie Cisco XDR domänenübergreifende Transparenz, Korrelation, Priorisierung, Untersuchung sowie koordinierte und automatisierte Reaktionen über integrierte

Sicherheitskontrollen hinweg ermöglicht.

Weltweite Trainingscenter





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch