Implementing and Configuring Cisco Identity Services Engine (SISE)

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

Zielgruppe

- Netzwerksicherheitsingenieure
- Netzwerkadministratoren
- Beratende Sicherheitsingenieure
- Technische Lösungsarchitekten
- Netzwerkmanager
- Vertriebsingenieure
- Kundenbetreuer

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Network Professional Security (CCNP SECURITY)

Voraussetzungen

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

- Vertrautheit mit der Cisco IOS® Software-Befehlszeilenschnittstelle (CLI) für kabelgebundene und kabellose Geräte
- Vertrautheit mit Cisco Secure Client
- Vertrautheit mit Microsoft Windows-Betriebssystemen
- Vertrautheit mit 802.1X

Diese Fähigkeiten finden Sie im folgenden Cisco-Lernangebot:

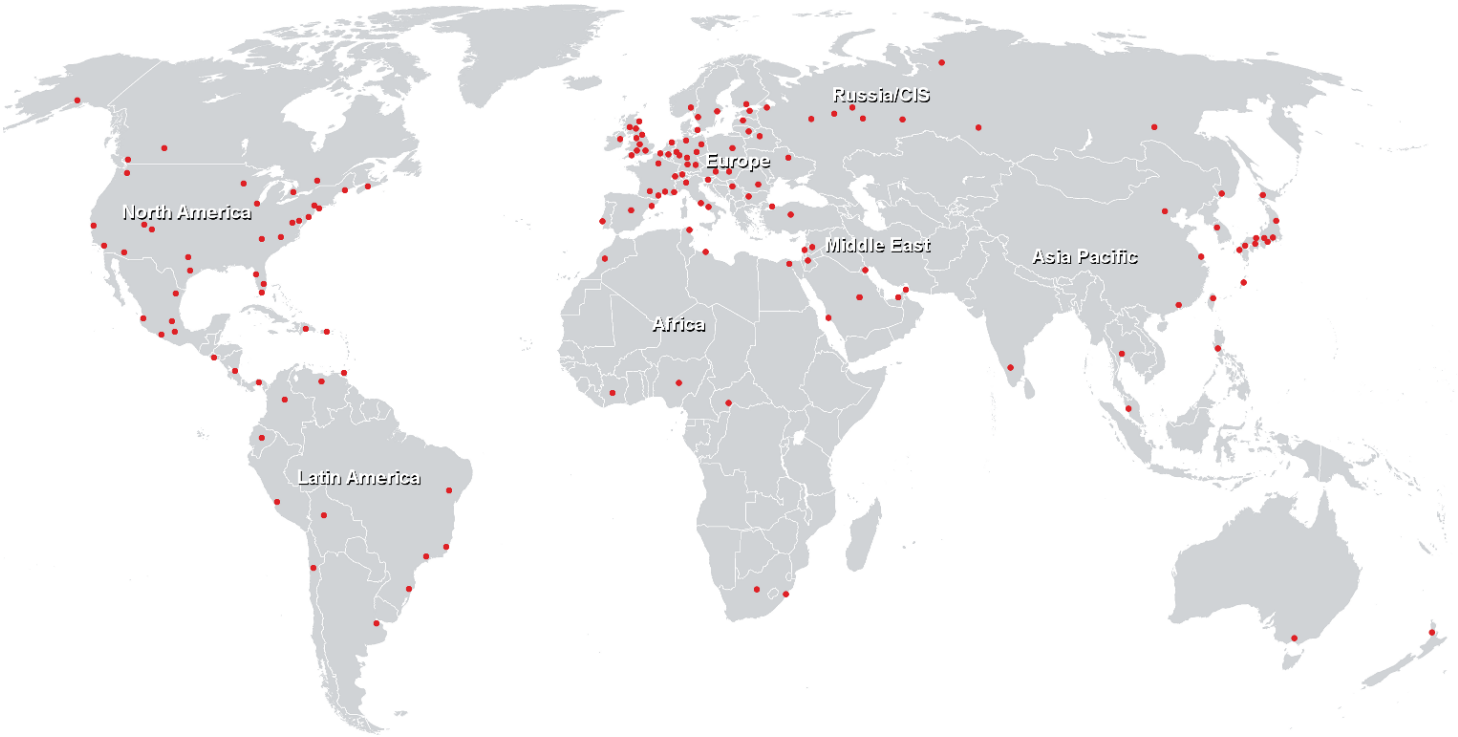
- Implementing and Operating Cisco Security Core Technologies (SCOR)

Kursziele

- Beschreiben Sie, wie Cisco ISE in moderne Netzwerksicherheitsarchitekturen passt, und erläutern Sie die Hauptfunktionen, die Gründe für das Design und häufige Anwendungsfälle.
- Untersuchen Sie die funktionalen Rollen der Cisco ISE-Knoten-Personas, die unterstützten Bereitstellungsmodelle, Lizenzierungsaspekte und deren Auswirkungen auf die Designplanung und Skalierbarkeitsentscheidungen.
- Implementieren Sie die Installationsabläufe, Plattformanforderungen und ersten Einrichtungsschritte für die Bereitstellung von Cisco ISE auf unterstützten virtuellen und Hardware-Plattformen.
- Bewerten Sie die Prinzipien, den Nachrichtenfluss und die Autorisierungsergebnisse des 802.1X-basierten Netzwerkzugangs sowie den Beitrag von Cisco ISE zur Sicherheit von kabelgebundenen und kabellosen Verbindungen mit identitätsbasierten Kontrollen.
- Beschreiben Sie, wie MAB funktioniert, einschliesslich seines Fallback-Verhaltens, seiner Ablaufsequenz und der Richtlinienanwendung innerhalb von Cisco ISE, und wie MAB den Zugriff auf nicht 802.1X-kompatible Geräte ermöglicht.
- Legen Sie die Rolle von NADs in Cisco ISE-Authentifizierungs-Workflows fest und geben Sie einen Überblick über die erforderlichen Schritte zum Hinzufügen, Konfigurieren und Validieren von NADs innerhalb von Cisco ISE, um eine sichere Durchsetzung von Richtlinien zu gewährleisten.
- Erörtern Sie die Rolle interner und externer Identitätsquellen in Cisco ISE, wie Benutzer- und Geräteidentitäten verwaltet werden und wie Zertifikate für die identitätsbasierte Authentifizierung verwendet werden.
- Bewerten Sie, wie Cisco ISE für die Integration mit Active Directory und LDAP konfiguriert werden muss, und beschreiben Sie die wichtigsten Einstellungen und Konnektivitätsanforderungen, die zur Unterstützung der externen Benutzerauthentifizierung erforderlich sind.
- Erläutern Sie, wie Cisco ISE Identitätsquellen während der Authentifizierung auswählt, und beschreiben Sie die Logik und Bedingungen, die die Reihenfolge der Identitätsspeicher, das Fallback-Verhalten und die Techniken zur Identitätsnormalisierung bestimmen.
- Besprechen Sie die Struktur und den Zweck von Richtliniensätzen in Cisco ISE, einschliesslich der Interaktion zwischen globalen und lokalen Konstrukten, der Abgleichung und Bewertung von Richtliniensätzen sowie der Organisation der Authentifizierungs- und Autorisierungslogik innerhalb jedes Richtliniensatzes.
- Identifizieren Sie, wie Cisco ISE Authentifizierungsrichtlinien anhand von Regelbedingungen, Identitätsspeichersequenzen und Wörterbüchern bewertet und wie das Verhalten angewendet wird, wenn keine Regeln übereinstimmen.

- Interpretieren Sie, wie Cisco ISE nach der Authentifizierung Autorisierungsrichtlinien anwendet, einschliesslich der Erstellung von Regeln mit Conditions Studio und dem Abgleich mit Benutzer- und Geräteattributen, um geeignete Zugriffsprofile anzuwenden.
- Analysieren Sie Cisco ISE-Richtlinien auf der Grundlage von Protokollen, RADIUS-Flussdaten und Sitzungskontext, um Authentifizierungs- und Autorisierungsprobleme in verschiedenen Zugriffsszenarien zu lösen.
- Analysieren Sie, wie Cisco ISE mithilfe von CWA webbasierten Gastzugang bereitstellt, und unterscheiden Sie zwischen Hotspot-, Selbstregistrierungs- und gesponsertem Zugriff.
- Legen Sie globale Gästeeinstellungen in Cisco ISE fest, um das Verhalten während des Lebenszyklus von Konten, Richtlinien für Anmeldedaten, Kommunikationsmethoden und Zugriffstypen für Gäste in allen unterstützten Onboarding-Prozessen zu definieren.
- Konfigurieren Sie Cisco ISE-Gastportale, um verschiedene Zugriffsabläufe zu unterstützen, Kontolebenszyklen zu verwalten und Bereitstellungsmodelle zu implementieren, die mit den Richtlinien und Skalierbarkeitsanforderungen Ihres Unternehmens übereinstimmen.
- Richten Sie in Cisco ISE einen sponsorgesteuerten Gastzugang über Zugriffsrollen ein, indem Sie Gasttypen mit Sponsorengruppen verknüpfen und das Portalverhalten so anpassen, dass die Erstellung und Genehmigung von Konten unterstützt wird.
- Schaffen Sie ein klares Verständnis der Funktionen von Cisco ISE für einen sicheren und skalierbaren BYOD-Zugang: Anwendungsfälle in Unternehmen, Bereitstellungsmodelle, richtlinienbasierte Kontrollstrategien, Schlüsselkomponenten, Cisco ISE-spezifische Funktionen und Onboarding-Designs wie einzelne und doppelte SSIDs für die nahtlose Integration persönlicher Geräte in das Netzwerk.
- Konfigurieren Sie Cisco ISE so, dass es Supplicants bereitstellt, Zertifikate ausstellt und Richtlinien als Teil einer vollständigen BYOD-Onboarding-Pipeline durchsetzt.
- Verwaltung von Workflows nach der Onboarding-Phase über das My Device Portal, einschliesslich Widerruf von Zertifikaten und Abmeldung von Geräten bei Verlust oder Diebstahl von Endgeräten
- Erläutern Sie, wie Cisco ISE Profiling nutzt, um Endpunkte zu identifizieren, indem es Klassifizierungslogik, Profiler-Komponenten, Datenflüsse und Feed-Dienste nutzt, um die Grundlage für erweitertes Profiling und die Durchsetzung von Richtlinien zu schaffen.
- Analysieren Sie, wie Cisco ISE Endpunktdaten mithilfe integrierter Sonden, Gerätesensoren und pxGrid-Anreicherung erfasst und wie jede Methode zur Genauigkeit und Abdeckung der Profilerstellung beiträgt.
- Analysieren Sie, wie die Profiling-Richtlinien in Cisco ISE Endpunkte anhand von Erfassungsattributen klassifizieren und wie logische Profile erstellt und angewendet werden, um den Entscheidungsprozess zur Festlegung des Zugriffs auf der Grundlage der Identität zu unterstützen.
- Entwickeln Sie skalierbare Profiling-Lösungen, indem Sie Designprinzipien, Sondenauswahl und NAD-Integration auf verschiedene Netzwerkumgebungen abstimmen.
- Sorgen Sie für Transparenz bei der Profilerstellung durch Dashboards und Reporting-Tools und verbessern Sie die Effizienz der Bereitstellung durch Optimierungstechniken.
- Grundlegendes Verständnis der Cisco ISE-Posture-Services anwenden, einschliesslich Agententypen, Ablauflogik, Betriebsmodi und Anwendungsfälle
- Implementieren Sie Cisco ISE, um Posture-Agenten und zugehörige Ressourcen für Endgeräte bereitzustellen, indem Sie Aktualisierungsdienste, Portale und Bereitstellungsrichtlinien konfigurieren.
- Verwalten Sie Cisco ISE-Richtlinien, um einen sicheren und konformen Netzwerkzugriff zu gewährleisten.
- Testen Sie die durchsetzungsbasierte Zugriffskontrolle, indem Sie verschiedene Endpunktszenarien mit Cisco AnyConnect simulieren.
- Bewerten Sie das Verhalten während der Sitzung, interpretieren Sie die Ergebnisse der Körperhaltung und analysieren Sie die Berichterstattungsinstrumente, um die Wirksamkeit der Anwendung der Richtlinien zur Körperhaltung und der Abhilfemassnahmen zu bestätigen.
- Untersuchen Sie die Verwendung von TACACS+ durch Cisco ISE zur Sicherung des administrativen Zugriffs, einschliesslich wichtiger AAA-Konzepte und eines Vergleichs mit RADIUS, um die zentralisierte Authentifizierung und Autorisierung zu veranschaulichen.
- Richten Sie Cisco ISE für die TACACS+-basierte Geräteverwaltung ein, indem Sie Richtlinienelemente wie Befehlssätze, Profile und Richtliniensätze konfigurieren.
- Integrieren Sie Netzwerkgeräte, definieren Sie Zugriffsberechtigungen und richten Sie Authentifizierungs- und Autorisierungsregeln ein, um den Administratorzugriff zu kontrollieren.
- Implementieren Sie eine erweiterte TACACS+-Autorisierungslogik, implementieren Sie Administratorbefehlszugriff und implementieren Sie skalierbare Bereitstellungen unter Verwendung bewährter Designrichtlinien.
- Vergleichen Sie die Kernarchitektur, den Betrieb und die Designüberlegungen von Cisco TrustSec, einschliesslich der Verbesserungen und Planungsvoraussetzungen für den Einsatz in Unternehmen.
- Konfigurieren Sie die Cisco TrustSec-Segmentierung in Cisco ISE, einschliesslich SGT-Klassifizierung, SXP-Verbreitung und tagbasierter Durchsetzung von Richtlinien.
- Erläutern Sie, wie Cisco ISE durch Systemwartung, Sicherungs-/Wiederherstellungsverfahren, Zertifikatsverwaltung und strukturierte Upgrades in Produktionsumgebungen operationalisiert werden kann.

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