Implementing Automation for Cisco Security Solutions (SAUI)

ID SAUI **Prix** CHF 3 890,– (Hors Taxe) **Durée** 3 jours

A qui s'adresse cette formation

Ce cours est principalement destiné aux professionnels occupant des postes tels que :

- Ingénieur réseau
- Ingénieur systèmes
- Ingénieur sans fil
- Ingénieur systèmes consultant
- Architecte de solutions techniques
- Administrateur réseau
- Ingénieur en conception de réseaux sans fil
- Responsable réseau
- Ingénieur commercial
- Responsable de compte

Cette formation prépare à la/aux certifications

Cisco Certified Network Professional Security (CCNP SECURITY)
Cisco Certified DevNet Professional / CCNP Automation (CCDNP)

Pré-requis

Avant de vous inscrire à ce cours, vous devez avoir des connaissances professionnelles dans les domaines suivants :

- Concepts de base des langages de programmation
- Compréhension de base de la virtualisation
- Capacité à utiliser Linux et les outils de ligne de commande (CLI), tels que Secure Shell (SSH) et bash
- Connaissances de base en réseau au niveau CCNP
- Connaissances en sécurité des réseaux au niveau CCNP

Les cours Cisco suivants peuvent vous aider à acquérir les connaissances nécessaires pour vous préparer à ce cours :

- Implementing and Administering Cisco Solutions (CCNA)
- Introducing Automation for Cisco Solutions (CSAU)
- Implementing and Operating Cisco Security Core Technologies (SCOR)

Objectifs

Après avoir suivi ce cours, vous serez capable de :

- Décrire l'architecture globale des solutions de sécurité Cisco et comment les API permettent de renforcer la sécurité
- Savoir utiliser les API de Cisco Firepower
- Expliquer le fonctionnement des API pxGrid et leurs avantages
- Démontrer les capacités offertes par les API Cisco Stealthwatch et créer des requêtes API pour les modifications de configuration et les audits
- Décrire les fonctionnalités et les avantages de l'utilisation des API Cisco Stealthwatch Cloud
- Apprendre à utiliser l'API Cisco Umbrella Investigate
- Expliquer la fonctionnalité fournie par Cisco AMP et ses API
- Décrire comment utiliser les API Cisco Threat Grid pour analyser, rechercher et éliminer les menaces

Contenu

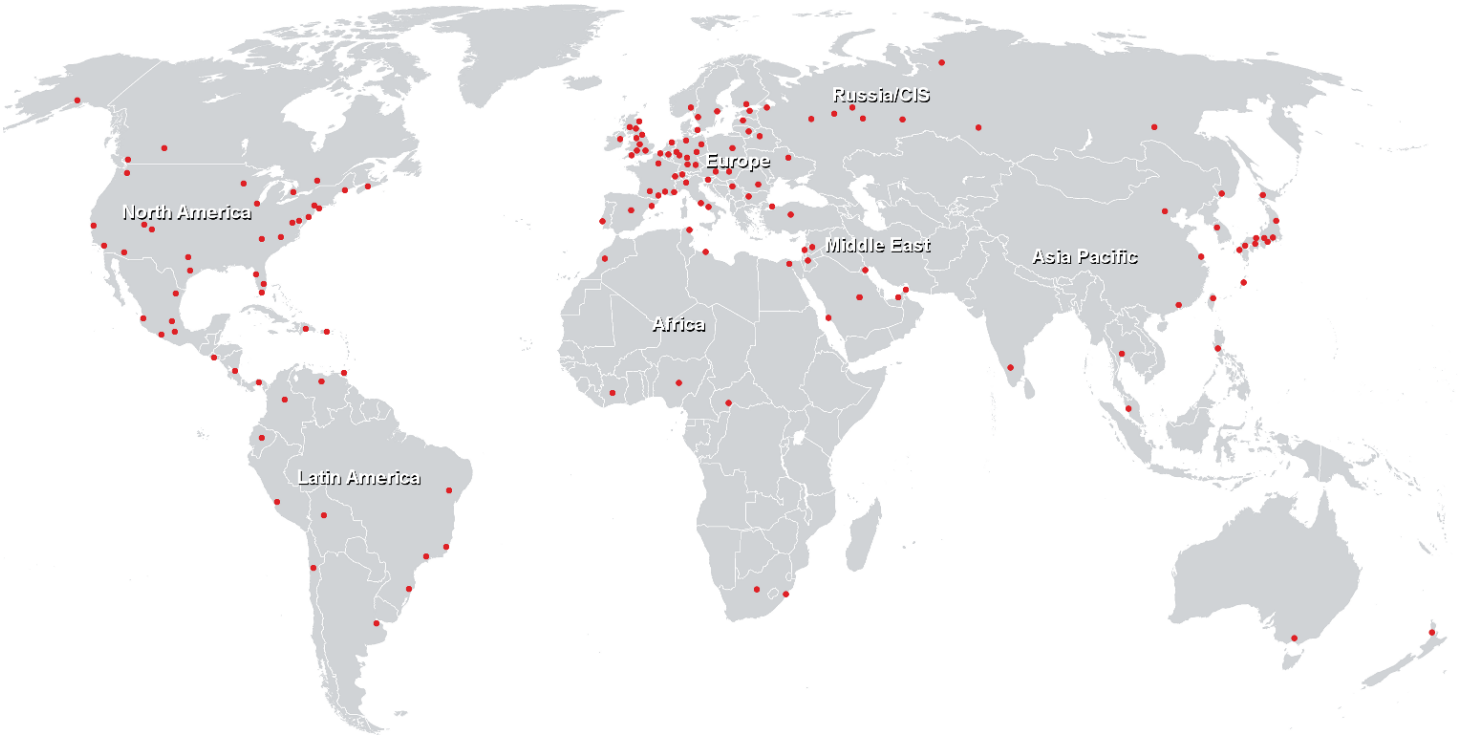
- Introduction aux API de sécurité Cisco
- Utilisation des API Cisco Advanced Malware Protection
- Utilisation de Cisco ISE
- Utilisation des API Cisco pxGrid
- Utilisation des API Cisco Threat Grid
- Investigation programmatique des données de sécurité Cisco Umbrella
- Exploration des API de reporting et d'application de Cisco Umbrella
- Automatisation de la sécurité avec les API Cisco Firepower
- Opérationnalisation de Cisco Stealthwatch et de ses capacités API
- Utilisation des API Cisco Stealthwatch Cloud
- Description des API de Cisco Security Management Appliance

Labs :

- Interroger les API Cisco AMP Endpoint pour vérifier la conformité
- Utiliser l'API REST et Cisco pxGrid avec Cisco Identity Services Engine
- Construire un script Python en utilisant l'API Cisco Threat Grid

- Générer des rapports en utilisant l'API de reporting de Cisco Umbrella
- Explorer l'API Cisco Firepower Management Center
- Utiliser Ansible pour automatiser la configuration de Cisco Firepower Threat Defense
- Automatiser les politiques de pare-feu en utilisant l'API Cisco Firepower Device Manager
- Automatiser les politiques d'alarme et créer des rapports en utilisant les API Cisco Stealthwatch
- Construire un rapport en utilisant les API Cisco Stealthwatch Cloud

Centres de formation dans le monde entier



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