Implementing and Operating Cisco Security Core Technologies (SCOR)

ID SCOR **Prix** CHF 4 150,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

- Ingénieurs en sécurité
- Ingénieurs réseaux
- Concepteurs réseaux
- Administrateurs réseaux
- Ingénieurs systèmes
- Ingénieurs systèmes consultants
- Architectes de solutions techniques
- Intégrateurs et partenaires Cisco
- Responsables réseaux
- Responsables de programmes
- Chefs de projet

Cette formation prépare à la/aux certifications

Cisco Certified Network Professional Security (CCNP SECURITY)
Cisco Certified Internetwork Expert (CCIE) Security (CCIE SECURITY)

Pré-requis

Il n'existe aucun prérequis formel pour cette formation. Toutefois, il est recommandé de posséder les connaissances et compétences suivantes avant d'y participer :

- Connaissance des réseaux Ethernet et TCP/IP
- Connaissance pratique du système d'exploitation Windows
- Connaissance pratique des concepts et du système d'exploitation réseau Cisco IOS
- Familiarité avec les concepts fondamentaux de la sécurité des réseaux

Ces compétences peuvent être acquises grâce à la formation Cisco suivante :

- Implementing and Administering Cisco Solutions (CCNA)

Objectifs

À l'issue de cette formation, vous serez capable de :

- Expliquer le mode de fonctionnement des différents acteurs de la menace en décrivant leurs motivations, leurs vecteurs d'attaque courants, les schémas typiques de compromission et d'abus d'identifiants, ainsi que le rôle du cycle de vie du renseignement sur les menaces cyber dans la compréhension et le suivi de ces menaces en constante évolution.
- Décrire comment les faiblesses structurelles des logiciels et applications web sont identifiées, classées et priorisées à l'aide de concepts tels que les classes de vulnérabilités, l'OWASP, les CVE et le CVSS, et expliquer comment les systèmes d'IA et les LLM élargissent ce paysage avec de nouveaux types de vulnérabilités.
- Expliquer pourquoi l'humain et l'identité demeurent des vecteurs d'attaque majeurs en décrivant les cycles de vie de l'ingénierie sociale et du vol d'identifiants, ainsi que les principales couches de défense mises en œuvre par les organisations pour réduire, sans toutefois éliminer complètement, les risques liés à l'identité.
- Décrire les principaux mécanismes cryptographiques : hachage, chiffrement symétrique et asymétrique, échange de clés, signatures numériques, PKI et protocoles de transport chiffrés, et expliquer les garanties de sécurité et hypothèses de confiance qu'ils apportent à une architecture d'entreprise.
- Expliquer comment les approches Zero Trust, défense en profondeur et le modèle Cisco SAFE Blueprint permettent de transformer les informations relatives aux menaces, vulnérabilités, identités et mécanismes cryptographiques en une architecture de sécurité cohérente qui suppose la défaillance, limite l'impact des incidents et guide le positionnement des technologies dans l'environnement.
- Décrire pourquoi le réseau d'accès de couche 2 constitue une frontière de sécurité fondamentale en expliquant comment la segmentation, la topologie, l'adressage, la découverte des voisins et les contrôles des ports d'accès contribuent à empêcher les attaques locales de compromettre la sécurité des couches supérieures.
- Décrire les méthodes de sécurisation des équipements d'infrastructure réseau en réduisant leur surface d'attaque, en protégeant les plans de gestion et de contrôle en tant que canaux d'autorité privilégiés, et en choisissant des architectures de gestion créant des frontières de confiance claires et défendables.
- Expliquer comment concevoir et exploiter une architecture

AAA (Authentication, Authorization and Accounting) pour l'administration de l'infrastructure en choisissant les protocoles appropriés, en définissant les comportements AAA et de repli, puis en dépannant méthodiquement les incidents AAA afin de restaurer un accès administratif sécurisé.
- Réaliser la configuration de base de Cisco Secure Firewall Threat Defense.
- Configurer une politique de contrôle d'accès avec politiques d'intrusion, de fichiers et anti-malware afin de répondre à des exigences de sécurité données.
- Configurer des solutions VPN site à site sécurisées afin d'établir une connectivité entre des sites distants à l'aide de Cisco Secure Firewall Threat Defense.
- Configurer des solutions VPN d'accès distant sur Cisco Secure Firewall Threat Defense afin de fournir une connexion sécurisée au réseau d'entreprise pour les utilisateurs distants.
- Évaluer les stratégies de sécurité cloud à l'aide des modèles de responsabilité partagée NIST 800-145, des cadres de sécurité et des solutions CASB dans des environnements multicloud.
- Décrire les stratégies de sécurisation des charges de travail cloud, y compris les principes de microsegmentation, Cisco Secure Workload, les plateformes Multicloud Defense et les approches de sécurité basées sur eBPF.
- Décrire les principes DevSecOps et Infrastructure as Code (IaC) et interpréter des scripts Python permettant d'appeler les API des équipements de sécurité.
- Décrire les architectures SASE (Secure Access Service Edge) et SSE (Security Service Edge), ainsi que les capacités de Cisco Secure Access pour fournir une protection unifiée dans le cloud des applications privées et d'Internet à travers les environnements distants et agences.
- Configurer une connectivité délivrée depuis le cloud, une authentification basée sur l'identité et des politiques d'accès granulaires afin de fournir un accès sécurisé aux applications privées pour les utilisateurs distants et en agence.
- Configurer la connectivité, l'identité et les contrôles de sécurité afin de fournir un accès sécurisé à Internet et aux applications SaaS pour les utilisateurs distants et en agence.
- Expliquer comment l'identité, le contexte des terminaux et le contrôle d'accès piloté par des politiques fonctionnent ensemble dans les solutions d'accès réseau sécurisé, et décrire comment Cisco ISE prend en charge des accès différenciés via AAA, l'accès invité, le profilage et le BYOD.
- Configurer le contrôle d'accès aux réseaux filaires et sans fil avec Cisco ISE en mettant en œuvre 802.1X et MAB, en appliquant les politiques d'authentification et d'autorisation Cisco ISE, en sélectionnant les méthodes EAP et supplicants appropriées, et en utilisant RADIUS et CoA afin d'appliquer les changements d'état d'accès.
- Expliquer comment Cisco Duo soutient les principes du Zero Trust grâce à une vérification renforcée des utilisateurs, la confiance des terminaux, des politiques d'accès adaptatives et une visibilité sur les risques identitaires via Cisco Identity Intelligence.
- Expliquer comment Cisco Secure Email Threat Defense est intégré et configuré dans les environnements de messagerie Microsoft 365 afin de fournir visibilité, analyse des menaces et remédiation contre le phishing, la fraude au président (BEC) et la compromission de comptes.
- Expliquer comment les organisations établissent, valident et appliquent la confiance des terminaux grâce à la gestion des équipements, la visibilité des actifs, l'évaluation de conformité et de posture, ainsi que le contrôle applicatif, afin de réduire les risques de sécurité des postes de travail.
- Expliquer comment les solutions modernes de sécurité des terminaux, telles que Cisco Secure Endpoint associé à Cisco Secure Malware Analytics, combinent prévention, détection continue, analyse des malwares et investigation pilotée par les événements à travers les concepts EPP (Endpoint Protection Platform) et EDR (Endpoint Detection and Response).
- Décrire le fonctionnement de Splunk Enterprise et Splunk Cloud en tant que plateformes d'analyse de données pour les opérations de sécurité, expliquer comment leurs composants et modèles de déploiement prennent en charge un traitement et une analyse évolutifs des données, construire des requêtes à l'aide du Splunk Processing Language pour rechercher et analyser les données collectées, expliquer l'intégration des produits de sécurité Cisco dans Splunk et décrire comment Splunk Enterprise étend la plateforme avec des capacités SIEM.
- Expliquer comment Splunk SOAR soutient les opérations SOC grâce à l'orchestration, l'automatisation via des playbooks et la réponse pilotée par les cas, et décrire son fonctionnement avec Splunk Enterprise Security et Cisco XDR pour automatiser les workflows d'investigation et de réponse.
- Expliquer comment le XDR unifie la détection, l'investigation et la réponse aux menaces à travers plusieurs domaines de sécurité, et décrire comment Cisco XDR fournit visibilité transverse, corrélation, priorisation, investigation et réponse coordonnée et automatisée au travers de contrôles de sécurité intégrés.

Contenu

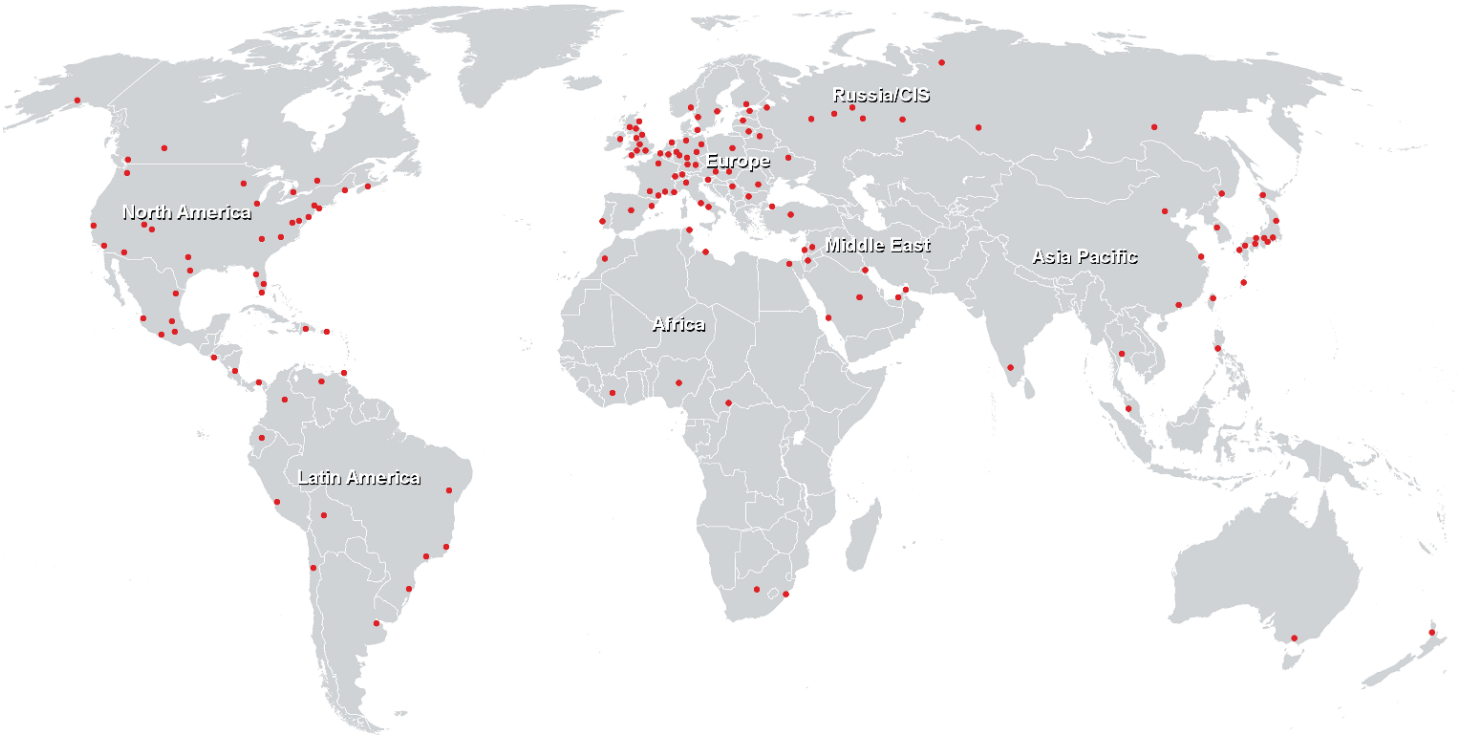
- Analyse et renseignement modernes sur les cybermenaces
- Vulnérabilités, exploits et risques liés à l'IA
- Ingénierie sociale, abus d'identités et contrôles anti-phishing

- Fondamentaux de la cryptographie
- Sécurité de la couche 2
- Principes de conception : Zero Trust et SAFE
- Renforcement de la sécurité des équipements et gestion sécurisée
- Dépannage AAA pour l'administration des équipements
- Déploiement de Cisco Secure Firewall Threat Defense
- Politiques de sécurité Cisco Secure Firewall
- Solutions VPN site à site
- Solutions VPN d'accès distant
- Modèles et cadres de sécurité cloud
- Charges de travail cloud sécurisées et eBPF
- DevSecOps et automatisation de la sécurité
- Zero Trust Identity avec Cisco Duo
- Architecture SASE et SSE
- Mise en œuvre d'un accès privé sécurisé
- Mise en œuvre d'un accès Internet sécurisé
- Principes fondamentaux de la gestion des identités et des accès
- Configuration de 802.1X, MAB et CoA avec Cisco ISE
- Cisco Secure Email Threat Defense (ETD)
- Confiance des terminaux, conformité et gestion des équipements
- EDR moderne et analyse des malwares
- Splunk et l'analyse de sécurité
- Automatisation SOC et SOAR
- Extended Detection and Response (XDR)

Labs

- Renforcement de la sécurité des équipements Cisco IOS XE
- Authentification du protocole de routage OSPFv3
- Administration des équipements réseau avec TACACS+
- Configuration initiale de Cisco Secure Firewall
- Gestion des politiques de sécurité Cisco Secure Firewall
- VPN site à site avec Cisco Secure Firewall
- VPN d'accès distant avec Cisco Secure Firewall
- Mise en œuvre d'un accès privé sécurisé (Secure Private Access)
- Mise en œuvre d'un accès Internet sécurisé (Secure Internet Access)
- MAB et 802.1X filaire avec Cisco ISE
- Cisco Secure Email Threat Defense
- Cisco Secure Endpoint
- Intégration de Cisco Secure Firewall avec Splunk
- Cisco XDR

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