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

- Ingénieur sécurité
- Ingénieur réseau
- Concepteur réseau
- Administrateur réseau
- Ingénieur système
- Ingénieur en systèmes de conseil
- Architecte des solutions techniques
- Intégrateurs/partenaires Cisco
- Gestionnaire de réseau
- Intégrateurs et partenaires de Cisco

Cette formation prépare à la/aux certifications

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

Pré-requis

Pour profiter pleinement de ce cours, vous devriez posséder les connaissances et compétences suivantes :

- Des compétences et des connaissances équivalentes à celles acquises dans le cours Implementing and Administering Cisco Solutions (CCNA)
- Familiarité avec Ethernet et les réseaux TCP/IP
- Connaissance pratique du système d'exploitation Windows
- Connaissance pratique des réseaux et des concepts de Cisco IOS
- Familiarité avec les notions de base de la sécurité des réseaux

Objectifs

À l'issue de ce cours, vous serez capable de :

- Décrire les concepts et les stratégies de sécurité de l'information au sein du réseau
- Décrire les attaques courantes de TCP/IP, d'applications réseau et de points d'extrémité
- Décrire comment les différentes technologies de sécurité des réseaux fonctionnent ensemble pour se protéger contre les attaques
- Mettre en place un contrôle d'accès sur l'appliance Cisco ASA et le pare-feu Cisco Firepower de nouvelle génération
- Décrire et mettre en œuvre les fonctions de base de la sécurité du contenu du courrier électronique fournies par l'application Cisco Email Security Appliance
- Décrire et mettre en œuvre les caractéristiques et les fonctions de sécurité du contenu web fournies par le Cisco Web Security Appliance
- Décrire les capacités de sécurité de Cisco Umbrella, les modèles de déploiement, la gestion des politiques et la console Investigate
- Introduire les VPN et décrire les solutions et les algorithmes de cryptographie
- Décrire les solutions de connectivité sécurisée de point à point Cisco et expliquer comment déployer les VPN IPsec point à point basés sur le système IOS VTI de Cisco et les VPN IPsec point à point sur le Cisco ASA et le Cisco FirePower NGFW
- Décrire et déployer les solutions de connectivité d'accès à distance sécurisé Cisco et décrire comment configurer l'authentification 802.1X et EAP
- Fournir une compréhension de base de la sécurité des points d'accès et décrire l'architecture et les caractéristiques de base de l'AMP pour les points d'accès
- Examiner les différentes défenses des dispositifs Cisco qui protègent le plan de contrôle et de gestion
- Configurer et vérifier les contrôles des plans de données de la couche 2 et de la couche 3 du logiciel Cisco IOS
- Décrire les solutions Stealthwatch Enterprise et Stealthwatch Cloud de Cisco
- Décrire les principes de base de l'informatique en nuage et les attaques courantes dans le cloud, ainsi que la manière de sécuriser l'environnement cloud

Contenu

Description des concepts de sécurité de l'information*

- Aperçu de la sécurité de l'information
- Gestion des risques
- Évaluation de la vulnérabilité
- Comprendre CVSS

Description des attaques TCP/IP les plus courantes*

- Vulnérabilités de l'ancien TCP/IP
- Vulnérabilités IP
- Vulnérabilités ICMP
- Vulnérabilités TCP
- Vulnérabilités UDP
- Surface d'attaque et vecteurs d'attaque
- Attaques de reconnaissance
- Attaques d'accès
- Attaques de l'homme du milieu
- Attaques par déni de service et par déni de service distribué
- Attaques par réflexion et amplification
- Attaques d'usurpation d'identité
- Attaques DHCP

Description des attaques des applications de réseau les plus communes*

- Attaques reposant sur les mots de passe
- Attaques basées sur le DNS
- Tunnels DNS
- Attaques basées sur le Web
- HTTP 302 Cushioning
- Injections de commandes
- Injections SQL
- Scripting intersite et falsification de requête
- Attaques par courrier électronique

Description des attaques de points finaux les plus fréquentes*

- Débordement de mémoire tampon
- Logiciel malveillant
- Attaque de reconnaissance
- Obtenir l'accès et le contrôle
- Obtention d'un accès par ingénierie sociale
- Obtention d'un accès par le biais d'attaques basées sur le Web
- Kits d'exploitation et Rootkits
- Escalade des privilèges
- Phase de post-exploitation
- Kit d'exploitation Angler

Description des technologies de sécurité des réseaux

- Stratégie de défense en profondeur
- La défense à travers le continuum d'attaque
- Vue d'ensemble de la segmentation et de la virtualisation du réseau
- Pare-feu dynamique (Stateful Firewall)
- Aperçu des renseignements de sécurité
- Normalisation des informations sur les menaces
- Protection contre les logiciels malveillants en réseau
- Présentation de l'IPS
- Pare-feu de nouvelle génération
- Aperçu de la sécurité du contenu des courriels
- Présentation de la sécurité du contenu Web
- Systèmes d'analyse des menaces
- Présentation de la sécurité DNS
- Présentation de l'authentification, de l'autorisation et de la comptabilité
- Aperçu de la gestion des identités et des accès
- Aperçu de la technologie des réseaux privés virtuels
- Aperçu des facteurs de forme des dispositifs de sécurité des réseaux

Déploiement du pare-feu Cisco ASA

- Types de déploiement de Cisco ASA
- Niveaux de sécurité de l'interface Cisco ASA
- Objets et groupes d'objets de Cisco ASA
- Traduction d'adresses réseau
- ACLs d'interface Cisco ASA
- ACLs globales de Cisco ASA
- Politiques d'accès avancées de Cisco ASA
- Aperçu de la haute disponibilité de Cisco ASA

Déploiement du pare-feu de nouvelle génération Cisco Firepower

- Déploiements de Cisco Firepower NGFW
- Traitement des paquets et politiques de Cisco Firepower NGFW
- Objets Cisco Firepower NGFW
- Cisco Firepower NGFW NAT
- Politiques de préfiltrage de Cisco Firepower NGFW
- Politiques de contrôle d'accès de Cisco Firepower NGFW
- Intelligence de sécurité Cisco Firepower NGFW
- Politiques de découverte de Cisco Firepower NGFW
- Politiques d'IPS de Cisco Firepower NGFW
- Politiques de lutte contre les logiciels malveillants et de gestion des fichiers de Cisco Firepower NGFW

Déploiement de la sécurité du contenu des courriels

- Présentation de la sécurité du contenu des courriels de Cisco
- Présentation de SMTP
- Présentation de l'Email Pipeline
- Écoute publique et privée
- Présentation du tableau d'accès aux hôtes
- Présentation du tableau d'accès des destinataires
- Aperçu des politiques de courrier électronique
- Protection contre le spam et le courrier gris
- Protection contre les virus et les logiciels malveillants
- Filtres d'épidémie
- Filtres de contenu

- Prévention de la perte de données
- Chiffrement des courriels

Déploiement de la sécurité du contenu Web

- Présentation de Cisco WSA
- Options de déploiement
- Authentification des utilisateurs du réseau
- Décryptage du trafic HTTPS
- Politiques d'accès et profils d'identification
- Paramètres de contrôle d'utilisation acceptable
- Protection contre les logiciels malveillants

Déploiement de Cisco Umbrella*

- Architecture de Cisco Umbrella
- Déploiement de Cisco Umbrella
- Client itinérant de Cisco Umbrella
- Gestion de Cisco Umbrella
- Aperçu de l'enquête sur Cisco Umbrella

Présentation des technologies VPN et de la cryptographie

- Définition du VPN
- Types de VPN
- Communication sécurisée et services cryptographiques
- Clés en cryptographie
- Infrastructure à clé publique

Présentation des solutions VPN sécurisées de site à site de Cisco

- Topologies VPN site à site
- Vue d'ensemble des VPN IPsec
- Cartes cryptographiques statiques IPsec
- Interface de tunnel virtuel statique IPsec
- VPN multipoint dynamique
- Cisco IOS FlexVPN

Déploiement de l'IOS Cisco basé sur le VTI point à point

- Cisco IOS VTIs
- Configuration Static VTI Point-to-Point IPsec IKEv2 VPN

Déploiement de VPN IPsec point à point sur le Cisco ASA et le Cisco Firepower NGFW

- VPN point à point sur le Cisco ASA et le Cisco Firepower NGFW
- Configuration du VPN point à point du Cisco ASA
- Configuration du VPN point à point du Cisco Firepower NGFW

Présentation des solutions VPN d'accès distant sécurisé de Cisco

- Composants des réseaux privés virtuels d'accès à distance
- Technologies VPN d'accès à distance
- Vue d'ensemble de SSL

Déploiement de VPN SSL d'accès à distance sur le Cisco ASA et le Cisco Firepower NGFW

- Concepts de configuration de l'accès à distance
- Profils de connexion
- Stratégies de groupe
- Configuration du VPN d'accès à distance Cisco ASA
- Configuration du VPN d'accès à distance Cisco Firepower NGFW

Présentation des solutions d'accès sécurisé au réseau Cisco

- Accès au réseau sécurisé de Cisco
- Composants de l'accès réseau sécurisé de Cisco
- Rôle de l'AAA dans la solution Cisco Secure Network Access
- Moteur de services d'identité Cisco
- Cisco TrustSec

Description de l'authentification 8021X

- 802.1X et EAP
- Méthodes EAP
- Rôle de RADIUS dans les communications 802.1X
- Changement d'autorisation par RADIUS

Configuration de l'authentification 8021X

- Configuration du commutateur Cisco Catalyst 802.1X
- Configuration Cisco WLC 802.1X
- Configuration Cisco ISE 802.1X
- Configuration du Supplicant 802.1x
- Authentification Web centrale de Cisco

Description des technologies de sécurité des points d'accès*

- Pare-feu personnel basé sur l'hôte
- Anti-virus basé sur l'hôte
- Système de prévention des intrusions basé sur l'hôte
- Listes blanches et listes noires d'applications
- Protection contre les logiciels malveillants basée sur l'hôte
- Vue d'ensemble du sandboxing
- Contrôle de l'intégrité des fichiers

Déploiement de l'AMP Cisco pour les points d'extrémité*

- Architecture de Cisco AMP for Endpoints
- Moteurs Cisco AMP pour points finaux

- Sécurité rétrospective avec Cisco AMP
- Trajectoire des appareils et des fichiers Cisco AMP
- Gestion de Cisco AMP pour points finaux

Introduction à la protection des infrastructures de réseau*

- Identification des plans de dispositifs du réseau
- Contrôles de sécurité du plan de contrôle
- Contrôles de sécurité du plan de gestion
- Télémétrie du réseau
- Contrôles de sécurité du plan de données de la couche 2
- Contrôles de sécurité du plan de données de la couche 3

Déploiement des contrôles de sécurité dans les plans de contrôle*

- ACL d'infrastructure
- Police du plan de contrôle
- Protection du plan de contrôle
- Sécurité du protocole de routage

Déploiement des contrôles de sécurité du plan de données de la couche 2*

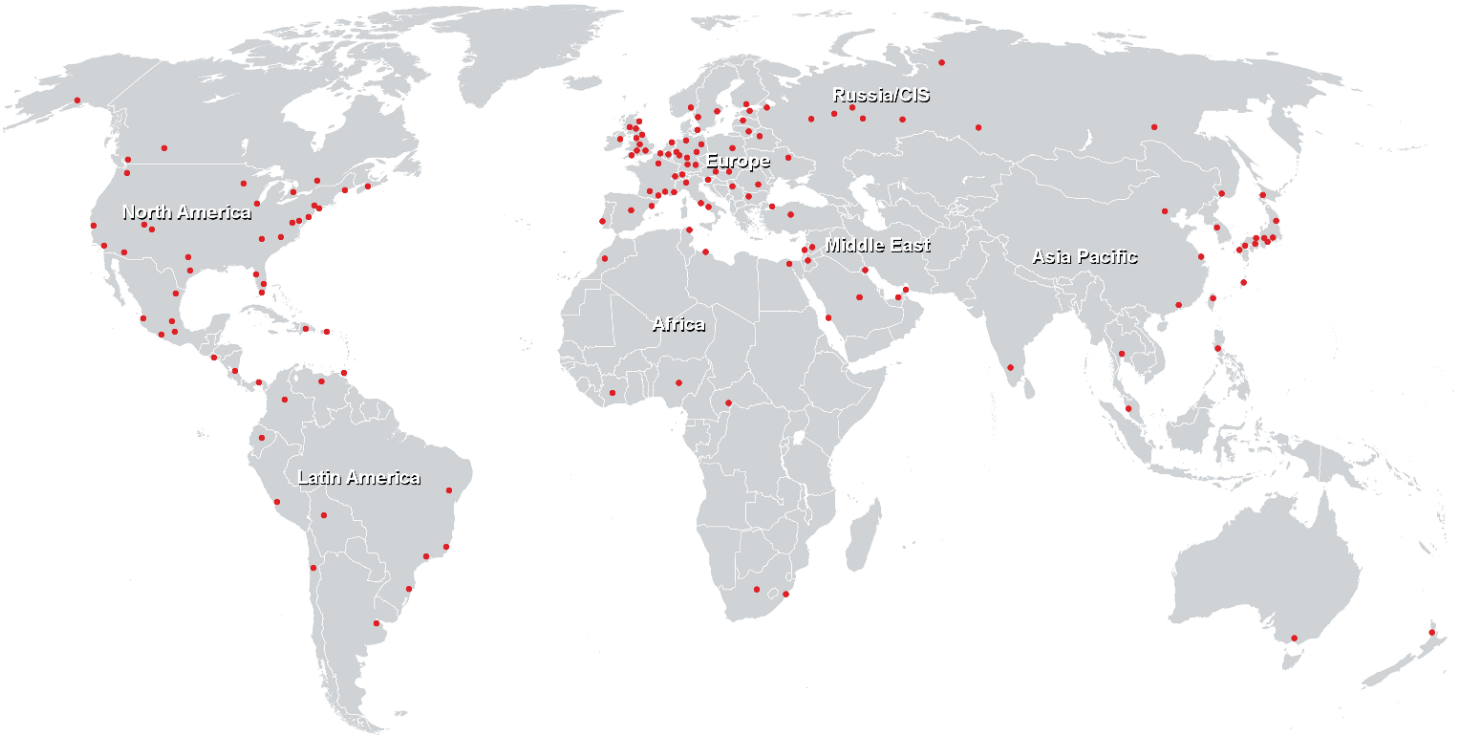
- Vue d'ensemble des contrôles de sécurité du plan de données de la couche 2
- Atténuation des attaques basées sur les réseaux locaux virtuels (VLAN)
- Atténuation des attaques STP
- Sécurité des ports
- VLAN privés
- L'espionnage DHCP
- Inspection ARP
- Contrôle STORM
- Cryptage MACsec

Déploiement des contrôles de sécurité du plan de données de la couche 3*

- ACL d'infrastructure contre l'usurpation (Antispoofing)
- Transfert de chemin inverse de l'unicast
- Protection de la source IP

* Cette section est du matériel d'auto-apprentissage qui peut être fait à votre propre rythme si vous suivez la version avec instructeur de ce cours

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer GmbH

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

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