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 réseau
- Designers réseau
- Administrateurs réseau
- Ingénieurs systèmes
- Ingénieurs systèmes de conseil
- Architectes de solutions techniques
- Intégrateurs et partenaires Cisco
- Responsables réseau
- Responsables de programme
- Chefs de projet

Cette formation prépare à la/aux certifications

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

Pré-requis

Il n'y a pas de prérequis formels pour cette formation. Cependant, les connaissances et compétences que vous êtes conseillé d'avoir avant d'assister à cette formation sont :

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

Ces compétences peuvent être trouvées dans l'offre de formation Cisco suivante :

- Implementing and Administering Cisco Solutions (CCNA)

Objectifs

Après avoir suivi ce cours, vous devriez être capable de :

- Décrire les concepts et stratégies de sécurité de l'information au sein du réseau
- Décrire les failles de sécurité dans le protocole de transmission/protocole Internet (TCP/IP) et comment elles peuvent être utilisées pour attaquer des réseaux et des hôtes
- Décrire les attaques basées sur les applications réseau
- Décrire comment diverses technologies de sécurité réseau travaillent ensemble pour se protéger contre les attaques
- Mettre en œuvre le contrôle d'accès sur le Cisco Secure Firewall Adaptive Security Appliance (ASA)
- Déployer les configurations de base du Cisco Secure Firewall Threat Defense
- Déployer les politiques de protection contre les menaces, les logiciels malveillants et les incendies du Cisco Secure Firewall Threat Defense
- Déployer les configurations de base du Cisco Secure Email Gateway
- Déployer les configurations de politiques du Cisco Secure Email Gateway
- Décrire et mettre en œuvre les fonctionnalités et fonctions de sécurité de contenu web de base fournies par le Cisco Secure Web Appliance
- Décrire diverses techniques d'attaque contre les points de terminaison
- Décrire les capacités de sécurité de Cisco Umbrella®, les modèles de déploiement, la gestion des politiques et la console d'investigation
- Fournir une compréhension de base de la sécurité des points de terminaison et être familiarisé avec les technologies de sécurité des points de terminaison courantes
- Décrire l'architecture et les fonctionnalités de base de Cisco Secure Endpoint
- Décrire les solutions Cisco Secure Network Access
- Décrire l'authentification 802.1X et le protocole d'authentification extensible (EAP)
- Configurer les appareils pour les opérations 802.1X
- Introduire les VPN et décrire les solutions et algorithmes de cryptographie
- Décrire les solutions de connectivité sécurisée site à site de Cisco
- Déployer des VPN IPsec point à point basés sur l'interface de tunnel virtuel (VTI) de Cisco Internetwork Operating System (Cisco IOS®)
- Configurer des VPN IPsec point à point sur le Cisco Secure

Firewall ASA et le Cisco Secure Firewall Threat Defense
- Décrire les solutions de connectivité sécurisée pour l'accès à distance de Cisco
- Déployer des solutions de connectivité sécurisée pour l'accès à distance de Cisco
- Fournir un aperçu des contrôles de protection de l'infrastructure réseau
- Examiner diverses défenses sur les appareils Cisco qui protègent le plan de contrôle
- Configurer et vérifier les contrôles du plan de données de couche 2 du logiciel Cisco IOS
- Configurer et vérifier les contrôles du plan de données de couche 3 du logiciel Cisco IOS et du Cisco ASA
- Examiner diverses défenses sur les appareils Cisco qui protègent le plan de gestion
- Décrire les formes de télémétrie de base recommandées pour les infrastructures réseau et les dispositifs de sécurité
- Décrire le déploiement de Cisco Secure Network Analytics
- Décrire les bases de l'informatique en cloud et des attaques cloud courantes
- Décrire comment sécuriser un environnement cloud
- Décrire le déploiement de Cisco Secure Cloud Analytics
- Décrire les bases des réseaux définis par logiciel et de la programmabilité des réseaux

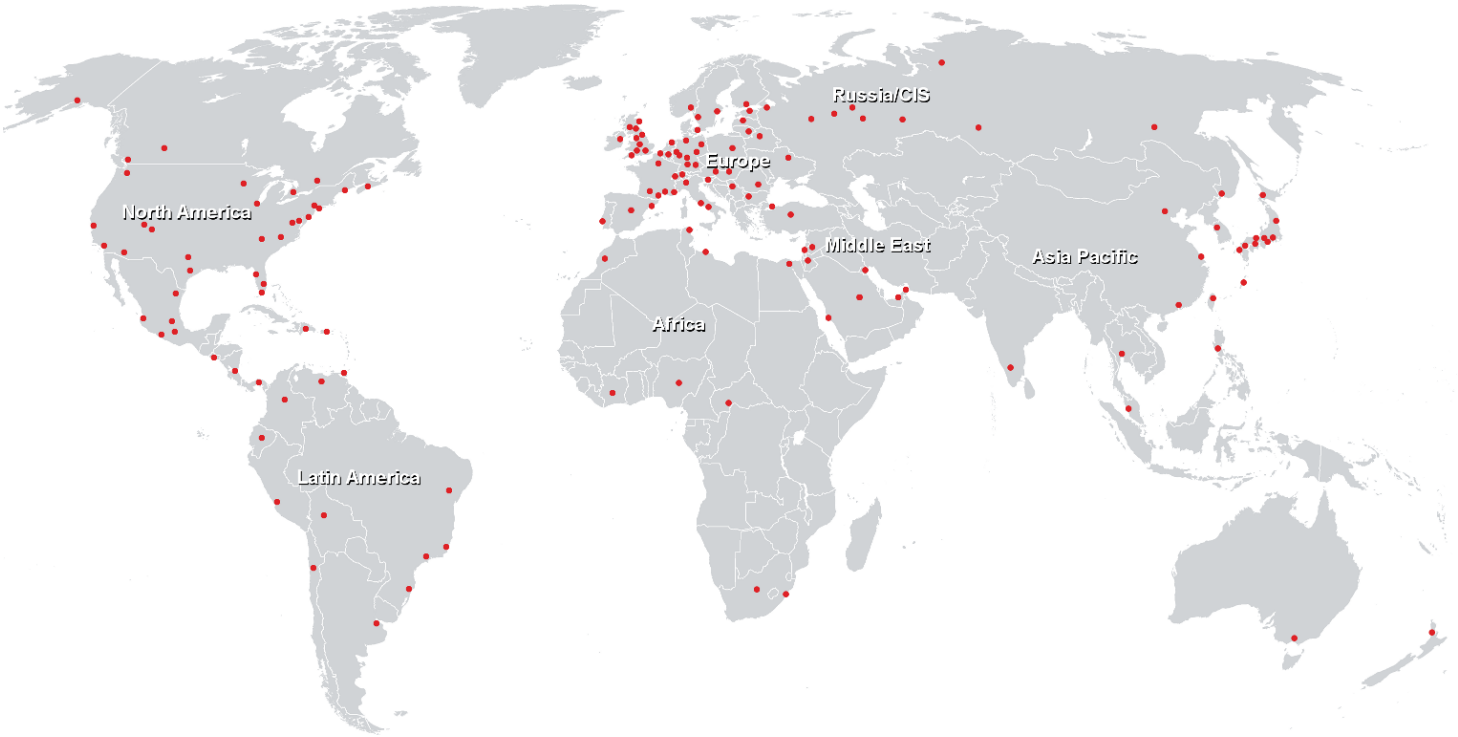
Contenu

- Technologies de sécurité réseau
- Déploiement de Cisco Secure Firewall ASA
- Notions de base de Cisco Secure Firewall Threat Defense
- IPS, politiques de malware et de fichiers de Cisco Secure Firewall Threat Defense
- Notions de base de Cisco Secure Email Gateway
- Configuration des politiques de messagerie sécurisée de Cisco
- Déploiement de Cisco Secure Web Appliance
- Technologies VPN et concepts de cryptographie
- Solutions de VPN site à site sécurisé de Cisco
- VPN IPsec point à point basé sur VTI Cisco IOS
- VPN IPsec point à point sur Cisco Secure Firewall ASA et Cisco Secure Firewall Threat Defense
- Solutions de VPN d'accès à distance sécurisé de Cisco
- VPN SSL d'accès à distance sur Cisco Secure Firewall ASA et Cisco Secure Firewall Threat Defense
- Description des concepts de sécurité de l'information
- Décrire les attaques TCP/IP courantes
- Décrire les attaques d'applications réseau courantes
- Attaques de point de terminaison courantes
- Déploiement de Cisco Umbrella
- Technologies de sécurité des points de terminaison
- Cisco Secure Endpoint
- Solutions de sécurité d'accès réseau de Cisco
- Authentification 802.1X
- Configuration de l'authentification 802.1X
- Protection de l'infrastructure réseau
- Solutions de sécurité du plan de contrôle
- Contrôles de sécurité du plan de données de couche 2
- Contrôles de sécurité du plan de données de couche 3
- Contrôles de sécurité du plan de gestion
- Méthodes de télémétrie du trafic
- Déploiement de Cisco Secure Network Analytics
- Informatique en nuage et sécurité du cloud
- Sécurité du cloud
- Déploiement de Cisco Secure Cloud Analytics
- Réseautage défini par logiciel

Labs

- Configurer les paramètres réseau et NAT sur Cisco Secure Firewall ASA
- Configurer les politiques de contrôle d'accès de Cisco Secure Firewall ASA
- Configurer le NAT de Cisco Secure Firewall Threat Defense
- Configurer la politique de contrôle d'accès de Cisco Secure Firewall Threat Defense
- Configurer la découverte et la politique IPS de Cisco Secure Firewall Threat Defense
- Configurer la politique de malware et de fichiers de Cisco Secure Firewall Threat Defense
- Configurer Listener, HAT et RAT sur Cisco Email Secure Email Gateway
- Configurer les politiques de messagerie sécurisée de Cisco
- Configurer les services proxy, l'authentification et le déchiffrement HTTPS
- Faire respecter le contrôle d'utilisation acceptable et la protection contre les malwares
- Configurer un tunnel IPsec IKEv2 point à point VTI statique
- Configurer un VPN point à point entre les dispositifs Cisco Secure Firewall Threat Defense
- Examiner le tableau de bord de Cisco Umbrella et la sécurité DNS
- Examiner le passerelle Web sécurisée de Cisco Umbrella et le pare-feu livré par le cloud
- Explorer les fonctionnalités CASB de Cisco Umbrella
- Explorer Cisco Secure Endpoint
- Effectuer une analyse des points de terminaison à l'aide de la console Cisco Secure Endpoint
- Explorer la protection contre les ransomwares de fichiers via la console Cisco Secure Endpoint
- Explorer Secure Network Analytics v7.4.2
- Explorer l'intégration des alertes mondiales de menaces et l'audit cryptographique ETA
- Explorer le tableau de bord et les opérations d'analyse du cloud
- Explorer la surveillance des clouds privés et publics sécurisés

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