Securing Email with Cisco Email Security Appliance (SESA)

ID SESA **Prix** CHF 3 630,– (Hors Taxe) **Durée** 4 jours

A qui s'adresse cette formation

- Ingénieurs en sécurité
- Administrateurs de sécurité
- Architectes de sécurité
- Ingénieurs d'exploitation
- Ingénieurs réseau
- Administrateurs réseau
- Techniciens réseau ou sécurité
- Gestionnaires de réseau
- Concepteurs de systèmes
- Intégrateurs et partenaires Cisco

Cette formation prépare à la/aux certifications

Cisco Certified Network Professional Security (CCNP SECURITY)

Pré-requis

Les compétences techniques de base que vous êtes censé avoir avant de suivre cette formation sont les suivantes :

- Certification Cisco, telle que la certification Cisco Certified Support Technician (CCST) en cybersécurité ou supérieure
- Certification industrielle pertinente, telle que (ISC)², CompTIA Security+, EC-Council, Global Information Assurance Certification (GIAC) et ISACA
- Attestation de fin de formation de Cisco Networking Academy (CCNA® 1 et CCNA 2)
- Expertise Windows, telle que Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE)], et CompTIA (A+, Network+, Server+)

Les connaissances et compétences que vous êtes censé avoir avant de suivre cette formation sont les suivantes :

- Services du protocole de contrôle de transmission/protocole internet (TCP/IP), y compris le système de noms de domaine (DNS), le shell sécurisé (SSH), le protocole de transfert de fichiers (FTP), le protocole simple de gestion de réseau (SNMP), le protocole de transfert hypertexte (HTTP) et le protocole de transfert hypertexte sécurisé (HTTPS)
- Expérience en routage IP

Objectifs

A l'issue de ce cours, vous devriez être capable de :

- Décrire et administrer le Cisco Email Security Appliance
- Contrôler les domaines des expéditeurs et des destinataires
- Contrôler le spam avec Talos SenderBase et l'anti-spam
- Utiliser les filtres antivirus et anti-outbreak
- Utiliser les politiques de messagerie
- Utiliser les filtres de contenu
- Utiliser les filtres de messages
- Prévenir la perte de données
- Effectuer des requêtes LDAP (Lightweight Directory Access Protocol)
- Authentifier les sessions SMTP (Simple Mail Transfer Protocol)
- Authentifier les emails
- Chiffrer les emails
- Utiliser les quarantaines systèmes et les méthodes de livraison
- Effectuer une gestion centralisée à l'aide de clusters
- Tester et dépanner

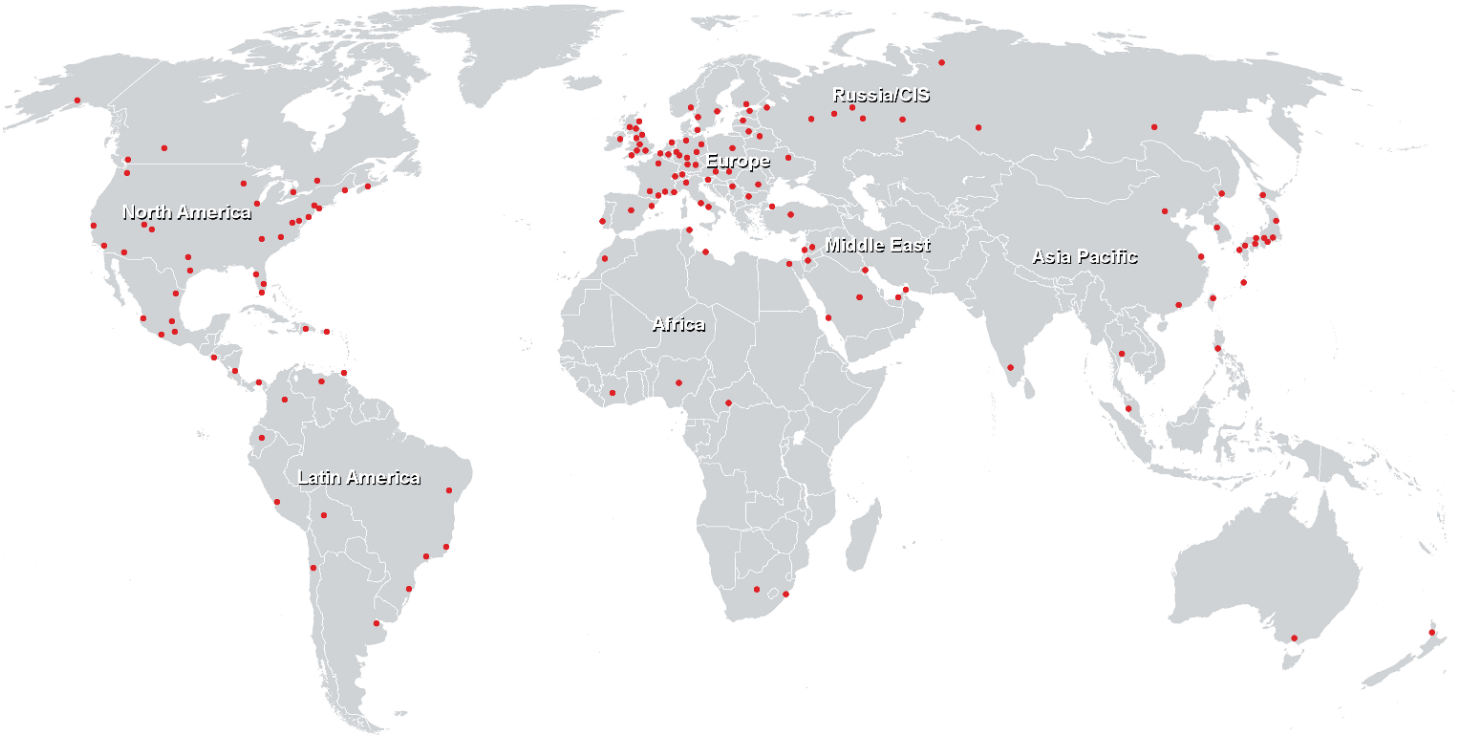
Contenu

- Description de Cisco Email Security Appliance
- Contrôle des domaines d'expéditeurs et de destinataires
- Contrôle du spam avec Talos SenderBase et anti-spam
- Utilisation des filtres anti-virus et de filtrage d'épidémies
- Utilisation des politiques de messagerie
- Utilisation des filtres de contenu
- Utilisation des filtres de messages
- Prévention des pertes de données
- Utilisation de LDAP
- Description de l'authentification des sessions SMTP
- Utilisation de l'authentification des emails
- Utilisation du chiffrement des emails
- Administration de Cisco Email Security Appliance
- Utilisation des quarantaines système et des méthodes de livraison
- Centralisation de la gestion à l'aide de clusters
- Tests et dépannage

Labs

- Vérifier et tester la configuration de Cisco ESA
- Détection avancée des malwares dans les pièces jointes (détection des macros)
- Protection contre les URLs malveillantes ou indésirables dissimulées sous des URLs raccourcies
- Protection contre les URLs malveillantes ou indésirables à l'intérieur des pièces jointes
- Gérer intelligemment les messages non scannables
- Exploiter l'intelligence cloud AMP via l'amélioration de pré-classification
- Intégrer Cisco ESA avec la console AMP
- Prévenir les menaces avec la protection anti-virus
- Appliquer des filtres d'épidémie
- Configurer le scan des pièces jointes
- Configurer la prévention des pertes de données sortantes
- Intégrer Cisco ESA avec LDAP et activer la requête d'acceptation LDAP
- Domain Keys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- Détection des emails falsifiés
- Effectuer l'administration de base
- Configurer le Cisco Secure Email and Web Manager pour le suivi et les rapports

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