

## Formation CISCO SESA, Sécuriser les emails avec Cisco Email Security Appliance

### Présentation

Cette formation prépare à la/aux certifications Cisco Certified Network Professional Security (CCNP SECURITY)

Durée : 35,00 heures (5 jours)

Tarif INTRA : Nous consulter

### Objectifs de la formation

- 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)
- Sécurisation du courrier électronique avec Cisco Email Security Appliance (SESA)
- 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
- Configurer le Cisco Secure Email and Web Manager pour le suivi et les rapports

### Prérequis

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)<sup>2</sup>, CompTIA Security+, EC-Council, Global Information Assurance Certification (GIAC) et ISACA
- Attestation de fin de formation de Cisco Networking Academy (CCNA<sup>®</sup> 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
- Il est nécessaire d'avoir une connaissance de l'anglais technique écrit pour la compréhension des supports de cours

## Public

- 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

## Programme de la formation

- 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

## Organisation

### Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances

techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

### **Moyens pédagogiques et techniques**

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

### **Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation**

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

## **Accessibilité**

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.