Sécuriser les emails avec Cisco Email Security Appliance

DURÉE
4 jours (28h)

RÉFÉRENCE
RST121

CATÉGORIE
Cisco Sécurité

OBJECTIFS DE LA FORMATION

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

- Pouvoir déployer et utiliser l'appliance Cisco® Email Security
- Dépanner et administrer l'appliance Cisco Email Security

POUR QUI ?

- Ingénieurs sécurité
- Administrateurs sécurité
- Architectes sécurité
- Ingénieurs opérationnels
- Ingénieurs réseau
- Administrateurs réseau
- Techniciens de réseau ou de sécurité
- Gestionnaires de réseaux
- Concepteurs de systèmes
- Intégrateurs et partenaires de Cisco

Programme détaillé

1/ Présentation du Cisco Email Security Appliance

- Vue d'ensemble de la technologie
- Cas d'usage
- Présentation technique de la technologie
- Vue d'ensemble du protocole SMTP
- Présentation du pipeline de messagerie

2/ Installer et configurer Cisco Email Security Appliance

- Scénarios d'installation
- Effectuer la configuration initiale du Cisco Email Security Appliance
- Centraliser les services sur un dispositif de gestion de la sécurité du contenu Cisco (SMA)
- Mise à jour pour AsyncOS

3/ Administrer Cisco Email Security Appliance

- Répartir les tâches administratives
- Administrer le système
- Gérer et surveiller l'aide de l'interface de ligne de commande (CLI)
- Autres tâches dans l'interface graphique
- Effectuer la cnfiguration avancée du réseau
- Utiliser Email Security Monitor
- Gestion et suivi des messages

- Logging

4/ Contrôler les domaines de l'expéditeur et du destinataire

- Auditeurs publics et privés
- Configurer gateway pour la réception de courriers électroniques
- Vue d'ensemble du Host Access Table
- Vue d'ensemble du Recipient Access Table
- Configurer les fonctions de routage et de transmission

5/ Contrôler le spam avec Talos SenderBase et Anti-Spam

- Vue d'ensemble de SenderBase
- Anti-Spam
- Gestion de Graymail
- Protection contre les URL malveillants ou indésirables
- Filtrer la réputation des fichiers et analyser les fichiers
- Vérifier les bounces

6/ Utiliser les filtres anti-virus et outbreaks

- Vue d'ensemble de l'analyse antivirus
- Effectuer le filtrage anti-virus Sophos
- Effectuer le filtrage anti-virus McAfee
- Configurer l'appareil pour la recherche de virus
- Appliquer les filtres d'outbreaks
- Vérifier le fonctionnement du dispositif de filtrage des outbreaks
- Gérer les filtres d'outbreaks

7/ Utiliser les politiques de courrier

- Vue d'ensemble du gestionnaire de sécurité du courrier électronique
- Vue d'ensemble des politiques en matière de courrier

- Traiter différemment les messages entrants et sortants
- Adapter les utilisateurs à une politique du courrier
- Déterminer les messages fractionnés
- Concevoir les politiques de courrier

8/ Réaliser le filtrage de contenus

- Vue d'ensemble des filtres de contenu
- Conditions de filtrage du contenu
- Actions de filtrage de contenu
- Filtrer les messages en fonction de leur contenu
- Vue d'ensemble des ressources textuelles
- Utiliser et tester les règles de filtrage des dictionnaires de contenu
- Comprendre les ressources textuelles
- Gérer les ressources textuelles
- Utiliser les ressources textuelles

9/ Utiliser les filtres de messages pour appliquer les stratégies de messagerie

- Vue d'ensemble des filtres de messages
- Présentation des composantes d'un filtre de messages
- Traiter les filtres de messages
- Définir les règles de filtrage des messages
- Appliquer les actions de filtrage des messages
- Numérisation des pièces jointes
- Présentation des exemples de filtres de messages pour l'analyse des pièces jointes
- Utiliser l'ICA (CLI) pour gérer les filtres de messages
- Présentation des exemples de filtres de messages
- Configurer le comportement de scan

10/ Création d'une politique de perte de données

- Identifier les problèmes de perte de données
- Vue d'ensemble de la solution Cisco DLP
- Mettre en œuvre la configuration DLP
- Présentation de RSA Engine

11/ Utiliser LDAP

- Présentation des fonctionnalités LDAP
- Utiliser les requêtes LDAP
- Authentifier des utilisateurs finaux de la quarantaine anti-spam
- Configurer l'authentification LDAP externe pour les utilisateurs
- Tester des serveurs et des requêtes
- Utiliser LDAP pour la prévention des attaques de répertoires
- Requêtes de consolidation d'alias de quarantaine pour les spams
- Valider les destinataires à l'aide d'un serveur SMTP

12/ Authentification de la session SMTP

- Configurer l’authentification AsyncOS pour SMTP
- Authentifier les sessions SMTP à l'aide de certificats de clients
- Vérifier la validité d'un certificat de client
- Authentifier un utilisateur à l'aide du répertoire LDAP
- Authentifier la connexion SMTP sur TLS
- Établir une connexion TLS à partir de l'appareil
- Mettre à jour une liste de certificats révoqués

13/ Authentification de l'email

- Vue d'ensemble de l'authentification du courrier électronique
- Configurer DomainKeys et signature du courrier identifié (DKIM)
- Vérifier les messages entrants à l'aide de DKIM
- Vue d'ensemble du cadre de la politique des expéditeurs (SPF) et vérification SIDF

- Vérifier la conformité et le rapport de conformité et d'authentification de message basée sur le domaine (DMARC)
- Vérifier le rapport d'authentification de message
- Vérifier la conformité (DMARC)
- Détecter les faux courriers

14/ Chiffrement d'Email

- Présentation de Cisco Email Encryption
- Cryptage des messages
- Déterminer les messages à chiffrer
- Insérer l’en-tête de chiffrement dans les messages
- Chiffrement des communications avec d'autres agents de transfert de messages (MTA)
- Travailler avec des certificats
- Gérer les listes d'autorités de certification
- Activer TLS sur une table d'accès à l'hôte d'un auditeur (HAT)
- Activation de la vérification TLS et du certificat à la livraison
- Services de sécurité S/MIME

15/ Elaborer et guider en quarantaines

- Présentation des quarantaines
- La quarantaine pour les spams
- Elaborer la quarantaine centralisée pour les spams
- Utiliser les listes de sécurité et les listes de blocage
- Configurer les fonctionnalités de gestion des spams pour les utilisateurs finaux
- Gérer les messages en quarantaine du courrier indésirable
- Mettre en quarantaine des stratégies, des virus et des épidémies
- Gérer la stratégie, les virus et les quarantaines épidémiques
- Utiliser les messages dans les stratégies, les virus ou les quarantaines épidémiques
- Méthodes de livraison

16/ Gestion centralisée à l'aide de clusters

- Vue d'ensemble de la gestion centralisée à l'aide des clusters
- Organisation du cluster
- Créer et rejoindre un cluster
- Gérer les clusters
- Communication des clusters
- Chargement d'une configuration dans les appareils en cluster
- Bonnes pratiques

17/ Tests et dépannage

- Identification des outils de dépannage
- Administrer le système

18/ Les références

- Spécifications du modèle pour les grandes entreprises
- Spécifications de modèle pour les entreprises moyennes et les petites ou moyennes entreprises ou les succursales
- Spécifications du modèle d'appareil Cisco Email Security pour les appareils virtuels
- Forfaits et licencess

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

02 au 05 Juin 2026	Casablanca - Maroc
28 au 31 Juil. 2026	Casablanca - Maroc
22 au 25 Sep. 2026	Casablanca - Maroc
17 au 20 Nov. 2026	Casablanca - Maroc

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-maroc.com
Web : https//www.innov-maroc.com

Scannez pour accéder à la fiche en ligne