Formation Sécuriser les emails avec Cisco Email Security Appliance (SESA)

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Référence	CS86
Durée	4 jours (28h)
Tarif	3 590 €HT

Objectifs

| mettre en oeuvre l'application Cisco de sécurité des mails
| intégrer un service d'annuaire via LDAP
| analyser et de réaliser le dépannage des problèmes d'intégration de LDAP
| utiliser les différents filtres afin de modifier et de réorienter les emails
| déployer en toute sécurité et réaliser le dépannage des filtres
| configurer TLS et le GSD (Guaranteed Secure Delivery)
| authentifier les emails à l'aide de DKIM et SPF
| Se préparer à passer l'examen Securing Email with Cisco Email Security Appliance (300-720 SESA)

Public

| Administrateurs systèmes
| Toute personne s'occupant de la messagerie (designers, architectes, gestionnaires réseaux...)

Prérequis

| Posséder des compétences et connaissances sur les fondamentaux TCP/IP (l'adressage IP et le sous-réseau, le routage statique IP et DNS)
| Posséder des compétences sur la messagerie internet (SNMTP, les formats de messages Internet et les formats de messages MIME)
| Connaitre et savoir manipuler l'interface en ligne de commandes (CLI) ainsi que l'interface graphique utilisateur (GU)
| Posséder des connaissances sur la sécurité des emails

Programme de la formation

Présentation de IronPort
| Présentation de la technologie et du produit
| Mettre en oeuvre et configurer IronPort

Organisation des mises en oeuvre
| Mettre en oeuvre et configurer le système
| Déterminer les expéditeurs ainsi que les groupes de destinataires

Paramétrer le public concerné
| Élaborer la stratégie de flux des messages
| Table d'accès des hôtes et des groupes de destinataires
| Routes SMTP
| Anti-Spam

Stopper les SPAMs à l'aide d'IronPorts
| Paramétrer et appliquer les sender base reputation scores ainsi que content adpative scanning engine
| Paramétrer et installer les Anti-Virus et Filtres
| Paramétrer l'activation d'un ou plusieurs Anti-Virus
| Appliquer les filtres contre les virus pour une protection Zerohour
| Utilisation des stratégies

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Concevoir des stratégies pour les mails des utilisateurs
| Déterminer les messages fractionnés
| Détailler la localisation centralisée (rapports
| Réaliser la localisation de messages

Élaborer et guider en quarantaines
| Consacrer des utilisateurs en quarantaine
| Attribuer des bounce profiles
| Élaborer des passerelles virtuelles
| Réaliser le filtrage de contenus

Détailler le scan des contenus
| Paramétrer la détection d'objet intégré
| Identifier les pièces jointes non protégées ou protégées par mot de passe
| Analyser des identifiants intelligents
| Crypter les messages

Le paramétrage d'une demande chiffrée
| Répondre avec le Cisco Registered Envelope Service
| Répondre avec un Serveur local de clés
| Dans une action de chiffrement lier une action de filtrage
| Paramétrer des demandes LDAP

Présentation de LDAP
| Jetons et opérateurs de demandes
| Paramétrer un profil LDAP ainsi que des Call-Ahead SMTP
| Appliquer les demandes groupées LDAP
| Routage LDAP et masquerading

Appliquer LDAP pour des demandes de routage des messages
| LDAP etpipe-line
| Paramétrer les demandes de routage
| Contrôler le routage LDAP
| Appliquer LDAP pour les requêtes déguisées
| Paramétrage du filtrage des messages

Présentation du filtrage des emails
| Overview
| Administrer le filtrage des messages
| Paramétrer TLS

Overview de TLS
| Paramétrer TLS
| Identification des emails

Résoudre les problèmes d'authentification
| Overview, signature et vérification DKIM
| Présentation de la technologie SPF et SIDF
| Vérification SPF

Analyser et séparer les problèmes
| Identification des outils de dépannage
| Administrer le système

Instruments pour le support
| Sauvegarder et restaurer le système
| Mettre à jour le logiciel

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.