Securing Email with Cisco Email Security Appliance (SESA) v3.2

Cours officiel, préparation à l'examen 300-720 SESA

Cours Pratique de 4 jours - 28h
Réf : LQN - Prix 2025 : 3 810 HT

Avec cette formation, vous déployez et utilisez Cisco Email Security Appliance pour protéger vos e-mails contre le phishing, les ransomwares et les compromissions. Vous apprenez à gérer les politiques de sécurité et à mettre en œuvre les principales fonctions : anti-spam, antivirus, filtrage des menaces, chiffrement, quarantaines et prévention des pertes de données. Vous développez vos compétences en déploiement, dépannage et administration de la solution.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Décrire et administrer le Cisco Email Security Appliance

Contrôler les domaines des expéditeurs et destinataires

Gérer le spam avec Talos SenderBase et l'anti-spam

Utiliser les filtres antivirus et de détection d'épidémies

Appliquer les politiques de messagerie

Utiliser les filtres de contenu

Utiliser les filtres de messages

Prévenir la perte de données

Effectuer des requêtes LDAP

Authentifier les sessions SMTP

Authentifier les e-mails

Chiffrer les e-mails

Gérer les quarantaines et les méthodes de livraison

Gérer de façon centralisée avec des clusters

Tester et dépanner

MÉTHODES PÉDAGOGIQUES

Animation de la formation en français. Support de cours officiel en anglais.

CERTIFICATION

Pour l'obtention de la certification Cisco Certified Network Professional Security (CCNP Security), la réussite de l'examen 350-701 SCOR est requise ainsi que la réussite de l'un des examens suivants (au choix) : 300-710 SNCF, 300-715 SISE, 300-720 SESA, 300-725 SWSA, 300-730 SVPN, 300-740 SCAZT ou 300-745 SDSI.

PARTICIPANTS

Ingénieurs, administrateurs, architectes et techniciens en sécurité ou réseau, ainsi qu'aux intégrateurs Cisco, partenaires, designers systèmes et responsables IT.

PRÉREQUIS

Bases solides en cybersécurité, protocoles réseau (DNS, SSH, FTP…) et une certification Cisco, CompTIA, (ISC)² ou expérience équivalente.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation…
À l'issue de chaque stage, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 06/2025

1) Programme officiel

- Présentation du Cisco Email Security Appliance.
- Contrôle des domaines d'expéditeurs et de destinataires.
- Lutte contre le spam avec Talos SenderBase et l'anti-spam.
- Utilisation des filtres antivirus et 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.
- Présentation de l'authentification des sessions SMTP.
- Utilisation de l'authentification des e-mails
- Utilisation du chiffrement des e-mails.
- Administration du Cisco Email Security Appliance.
- Utilisation des quarantaines et des méthodes de livraison.
- Centralisation de la gestion avec les clusters.
- Tests et dépannage.

2) Travaux pratiques officiels

- Vérifier et tester la configuration de Cisco ESA.
- Détection avancée de malwares dans les pièces jointes (macros).
- Protection contre les URL malveillantes ou indésirables cachées derrière des URL raccourcies.
- Protection contre les URL malveillantes ou indésirables dans les pièces jointes.
- Gestion intelligente des messages non analysables.
- Exploiter l'intelligence cloud AMP via l'amélioration de pré-classification.
- Intégrer Cisco ESA avec la console AMP.
- Prévenir les menaces avec la protection antivirus.
- Application des filtres d'épidémie.
- Configurer l'analyse des pièces jointes.
- Configurer la prévention des pertes de données en sortie.
- Intégrer Cisco ESA avec LDAP et activer la requête d'acceptation LDAP.
- Domain Keys Identified Mail (DKIM).
- Sender Policy Framework (SPF).
- Détection des e-mails falsifiés.
- Réaliser l'administration de base.
- Configurer Cisco Secure Email and Web Manager pour le suivi et les rapports.

LES DATES

CLASSE À DISTANCE	PARIS
2025 : 08 sept., 01 déc.	2025 : 01 sept., 24 nov.