Securing Email with Cisco Email Security Appliance (SESA) v3.1

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

Cours Pratique de 4 jours
Réf : LQN - Prix 2022 : 3 560€ HT

Avec cette formation "Sécuriser les emails avec Cisco Email Security Appliance", vous apprenez à déployer et à utiliser Cisco® Email Security Appliance pour établir la protection de vos systèmes de messagerie contre le phishing, la compromission de la messagerie professionnelle et les ransomwares. Vous apprenez aussi comment mettre en œuvre, dépanner et administrer Cisco Email Security Appliance, y compris des fonctionnalités clés telles que la protection avancée contre les logiciels malveillants, le blocage du courrier indésirable, la protection antivirus, etc.

OBJECTIFS PÉDAGOGIQUES

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

Décrire et administrer un Cisco Email Security Appliance (SESA)

Contrôler les domaines de l'expéditeur et du destinataire

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

Utiliser des filtres antivirus et outbreak

Utiliser les stratégies de messagerie

Utiliser des filtres de contenu

Utiliser des filtres de messages pour appliquer les politiques mails

Prévenir la perte de données

Effectuer des requêtes LDAP

Authentifier les sessions SMTP (Simple Mail Transfer Protocol)

Authentifier les e-mails

Crypter les e-mails

Utiliser des systèmes de quarantaine et des méthodes de diffusion

Effectuer une gestion centralisée à l'aide de 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 et 300-730 SVPN.

PARTICIPANTS

Ingénieurs sécurité, administrateurs sécurité, architectes sécurité, ingénieurs d'exploitation, ingénieurs réseau, administrateurs réseau, techniciens réseau ou sécurité, etc.

PRÉREQUIS

Connaissances de TCP/IP, DNS (Domain Name System), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP et HTTPS. Expérience du routage IP. Certifications requises.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont 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 cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• 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 stagiaire a bien assisté à la totalité de la session.

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 : 12/2021

1) Description du Cisco Email Security Appliance

- Présentation du Cisco Email Security Appliance.
- Fiche technique du Cisco Email Security Appliance.
- Présentation du SMTP.

- Vue d'ensemble de l'acheminement du courrier électronique.
- Scénarios d'installation.
- Configuration initiale du Cisco Email Security Appliance.
- Centralisation des services sur un dispositif de gestion de la sécurité du contenu Cisco (SMA).
- Notes de version pour AsyncOS 11.x.

2) Administration de Cisco Email Security Appliance

- Répartition des tâches administratives.
- Administration du système.
- Gestion et surveillance à l'aide de l'interface de ligne de commande (CLI).
- Autres tâches dans l'interface graphique.
- Configuration avancée du réseau.
- Utilisation d'Email Security Monitor.
- Suivi des messages.
- Logging.

3) Contrôle des domaines de l'expéditeur et du destinataire

- Auditeurs publics et privés.
- Configuration de la passerelle pour la réception de courriers électroniques.
- Présentation de la Host Access Table (HAT), la tâble d'accès des hôtes.
- Présentation de la Recipient Access Table (RAT), la table d'accès des destinataires.
- Configuration des fonctions de routage et de transmission.

4) Contrôle du spam avec Talos SenderBase et Anti-Spam

- Présentation de SenderBase.
- Anti-Spam.
- Gestion de Graymail.
- Protection contre les URL malveillantes ou indésirables.
- Filtrage de la réputation des fichiers et analyse des fichiers.
- Vérification des rebonds.

5) Utilisation des filtres antivirus et outbreaks

- Présentation de l'analyse antivirus.
- Filtrage antivirus Sophos.
- Filtrage antivirus McAfee.
- Configuration de l'appareil pour la recherche de virus.
- Filtres d'outbreaks.
- Fonctionnement du dispositif de filtrage des outbreaks.
- Gestion des filtres d'outbreaks

6) Utilisation des politiques de courrier

- Aperçu du gestionnaire de sécurité du courrier électronique.
- Aperçu des politiques en matière de courrier.
- Traiter différemment les messages entrants et sortants.
- Adaptation des utilisateurs à une politique du courrier.
- Fractionnement des messages.
- Configuration des politiques de courrier.

7) Utilisation des filtres de contenu

- Présentation des filtres de contenu.
- Conditions de filtrage du contenu.
- Actions de filtrage de contenu.
- Filtrage des messages en fonction du contenu.
- Aperçu des ressources textuelles.
- Utilisation et test des règles de filtrage des dictionnaires de contenu.

- Comprendre les ressources textuelles.
- Gestion des ressources textuelles.
- Utilisation des ressources textuelles.

8) Utilisation filtres de messages pour appliquer les stratégies de messagerie

- Présentation des filtres de messages.
- Composants d'un filtre de messages.
- Traitement du filtre de messages.
- Règles de filtrage des messages.
- Actions de filtrage des messages.
- Numérisation des pièces jointes.
- Exemples de filtres de messages d'analyse des pièces jointes.
- Utilisation de la CLI pour gérer les filtres de messages.
- Exemples de filtres de messages.
- Configuration du comportement d'analyse.

9) Prévention de la perte de données

- Présentation du processus d'analyse de la prévention des pertes de données (DLP).
- Configuration de la prévention contre la perte de données.
- Politiques de prévention de la perte de données.
- Actions sur les messages.
- Mise à jour du moteur DLP et des classificateurs de correspondance de contenu.

10) Utilisation de LDAP

- Présentation de LDAP.
- Travailler avec LDAP.
- Utilisation des requêtes LDAP.
- Authentification des utilisateurs finaux de la quarantaine de spam.
- Configuration de l'authentification LDAP externe pour les utilisateurs.
- Test des serveurs et des requêtes.
- Utilisation de LDAP pour la prévention des attaques par récolte d'annuaire.
- Requêtes de consolidation d'alias de quarantaine de spam.
- Validation des destinataires à l'aide d'un serveur SMTP.

11) Authentification de session SMTP

- Configuration d'AsyncOS pour l'authentification SMTP.
- Authentification des sessions SMTP à l'aide de certificats clients.
- Vérifier la validité d'un certificat client.
- Authentification de l'utilisateur à l'aide de l'annuaire LDAP.
- Authentification de la connexion SMTP sur Transport Layer Security (TLS) à l'aide d'un certificat client.
- Établissement d'une connexion TLS à partir de l'appliance.
- Mise à jour d'une liste de certificats révoqués.

12) Authentification par courriel

- Présentation de l'authentification par e-mail.
- Configuration de DomainKeys et de la signature DomainKeys Identified Mail (DKIM).
- Vérification des messages entrants à l'aide de DKIM.
- Présentation du Sender Policy Framework (SPF) et de la vérification SIDF.
- Vérification de la conformité et des rapports d'authentification de message basée sur le domaine (DMARC).
- Détection des e-mails falsifiés.

13) Cryptage des e-mails

- Présentation du chiffrement des e-mails Cisco.
- Cryptage des messages.

- Détermination des messages à chiffrer.
- Insertion d'en-têtes de chiffrement dans les messages.
- Cryptage de la communication avec d'autres agents de transfert de messages (MTA).
- Travail avec des certificats.
- Gestion des listes d'autorités de certification.
- Activation de TLS sur la table d'accès à l'hôte d'un écouteur (HAT).
- Activation de TLS et de la vérification de certificat à la livraison.
- Services de sécurité des extensions de messagerie Internet sécurisées/multifonctions (S/MIME).

14) Utilisation des quarantaines système et des méthodes de livraison

- Description des quarantaines.
- Quarantaine des spams.
- Configuration de la quarantaine centralisée du courrier indésirable.
- Utilisation de listes sécurisées et de listes de blocage pour contrôler la livraison des e-mails selon l'expéditeur.
- Configuration des fonctionnalités de gestion du courrier indésirable pour les utilisateurs finaux.
- Gestion des messages dans la quarantaine de spam.
- Quarantaines de stratégie, de virus et quarantaine.
- Gestion des politiques, des virus et des quarantaines.
- Travailler avec les messages dans les politiques, les virus ou les quarantaines.
- Méthodes de livraison.

15) Gestion centralisée à l'aide de clusters

- Présentation de la gestion centralisée à l'aide de clusters.
- Organisation de cluster.
- Création et fait de rejoindre un cluster.
- Gestion des clusters.
- Communication de cluster.
- Chargement d'une configuration dans les appareils en cluster.
- Meilleures pratiques.

16) Test et dépannage

- Débogage du flux de messagerie à l'aide de messages de test : trace.
- Utilisation de l'écouteur pour tester l'appareil.
- Dépannage du réseau.
- Dépannage de l'auditeur.
- Dépannage de la livraison des e-mails.
- Dépannage des performances.
- Aspect de l'interface web et problèmes de rendu.
- Réponses aux alertes.
- Dépannage des problèmes matériels.
- Travail avec le support technique.

17) Références

- Modèle de spécifications pour les grandes entreprises.
- Modèle de spécifications pour les entreprises de taille moyenne et les petites et moyennes entreprises ou succursales.
- Spécifications du modèle Cisco Email Security Appliance pour les appareils virtuels.
- Forfaits et licences.

18) Travaux pratiques officiels

- Vérifier et tester la configuration de Cisco Email Security Appliance (ESA).
- Effectuer l'administration de base.
- Comprendre le malware avancé dans les pièces jointes (détection de macro).
- Se protéger contre les URL malveillantes ou indésirables sous les URL raccourcies.

- Se protéger contre les URL malveillantes ou indésirables dans les pièces jointes.
- Gérer intelligemment les messages non scannables.
- Exploiter les renseignements du cloud AMP grâce à l'amélioration de la pré-classification.
- Intégrer Cisco ESA avec la console AMP.
- Prévenir les menaces avec la protection antivirus.
- Appliquer les filtres de contenu et d'outbreaks.
- Configurer la numérisation des pièces jointes.
- Configurer la prévention de la perte de données sortantes.
- Intégrer Cisco ESA avec LDAP et activer la requête d'acceptation LDAP.
- Activer la requête d'acceptation Lightweight Directory Access Protocol (LDAP).
- Comprendre le courrier identifié par les clés de domaine (DKIM).
- Sender Policy Framework (SPF).
- Détection des faux courriers électroniques.
- Configurer le Cisco SMA pour le suivi et les rapports.

LES DATES

PARIS LA DÉFENSE
2022 : 13 sept., 06 déc.

CLASSE A DISTANCE
2022 : 13 sept., 06 déc.