SECURING EMAIL WITH CISCO EMAIL SECURITY APPLIANCE

Cette formation vous montre comment déployer et utiliser le Cisco® Email Security Appliance pour établir la protection de vos systèmes de messagerie contre le phishing, la compromission des e-mails professionnels et les ransomwares, et pour vous aider à rationaliser la sécurité des e-mails et la gestion des politiques.

CURSUS:
CISCO

CODE DE LA FORMATION:
CS-SC-SESA

ÉDITEUR OU CONSTRUCTEUR:
CISCO

VERSION:
3.0

DURÉE:
3 JOURS

PRÉREQUIS:

Pour bénéficier pleinement de ce cours, vous devez disposer de l'une/plusieurs des compétences suivantes:

- Certification Cisco (Cisco CCENT® ou supérieure).
- Certification pertinente telle que (ISC) 2, CompTIA Security +, EC-Council, Global Information Assurance Certification (GIAC) et ISACA.
- Lettre de suivis du cursus Cisco Networking Academy (CCNA® 1 et CCNA 2).
- Expertise Windows: Microsoft [spécialiste Microsoft, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE)], CompTIA (A +, Network +, Server +).

Les connaissances et compétences qu'un stagiaire doit posséder avant de suivre ce cours sont:

- Services TCP/IP, y compris les protocoles: DNS, SSH, FTP, SNMP, HTTP et HTTPS.
- Expérience avec le routage IP.

PUBLIC:

Cette formation s'adresse aux:

- Ingénieurs Sécurité.
- Administrateurs Sécurité.
- Architecte Sécurité.
- Ingénieurs d'opération.
- Ingénieurs Réseau.
- Administrateurs Réseau.
- Techniciens Réseau ou Sécurité.
- Manager Réseau.
- Designers System.
- Intégrateurs et partenaires Cisco.

OBJECTIFS:

Après avoir suivi ce cours, vous devriez pouvoir:

- Décrire et administrer la Cisco Email Security Appliance (ESA).

- Contrôler les domaines de l’émetteur et du destinataire.
- Contrôlez le spam avec Talos SenderBase et anti-spam.
- Utiliser des filtres outbreak et antivirus.
- Utiliser les « mail policies ».
- Utiliser les « content filters ».
- Utiliser les « message filters » pour appliquer les « mail policies ».
- Empêcher la perte de données.
- Effectuer des requêtes LDAP.
- Authentifier les sessions SMTP.
- Authentifier les e-mails.
- Chiffrer les e-mails.
- Utiliser les quarantaines système et les méthodes de livraison.
- Effectuer une gestion centralisée à l'aide de clusters.
- Testez et dépannez.

CONTENU:

Décrire la solution Cisco Email Security Appliance

- Présentation du Cisco Email Security Appliance
- Cas d'utilisation de la technologie
- Fiche technique d Cisco Email Security Appliance
- Présentation du SMTP
- Présentation du pipeline de messagerie
- Scénarios d'installation
- Configuration initiale du Cisco Email Security Appliance
- Centralisation des services sur le Cisco Content Security Management Appliance(SMA)
- Notes de version pour AsyncOS 11.x

Administration du Cisco Email Security Appliance

- Distribution des tâches administratives
- L'administration du système
- Gestion et monitoring à l'aide de l'interface de ligne de commande (CLI)
- Autres tâches dans l'interface graphique
- Configuration réseau avancée
- Utilisation du Email Security Monitor
- Suivis des Messages
- Journalisation

Contrôle des domaines expéditeur et destinataire

- Listeners publics et privés
- Configuration de la passerelle pour recevoir des e-mails
- Présentation de la Host Access Table
- Présentation de la Recipient Access Table
- Configuration des fonctionnalités de routage et de livraison

Contrôle du spam avec Talos SenderBase et Anti-Spam

- Présentation du SenderBase
- Anti-spam
- Gérer les Graymails
- Protection contre les URL malveillantes ou indésirables
- Filtrage de la réputation des fichiers et analyse des fichiers
- Vérification du rebond

Utilisation des filtres outbreak et antivirus

- Présentation de l'analyse antivirus
- Filtrage antivirus Sophos
- Filtrage antivirus McAfee
- Configuration pour le scan des virus
- Filtres outbreak
- Fonctionnement du filtre outbeak
- Gestion des filtres outbreak

Utilisation des Mail Policies

- Présentation du Email Security Manager
- Présentation des Mail Policies
- Gestion différente des messages entrants et sortants
- Faire correspondre les utilisateurs à une Mail Polciy
- Éclatement de message
- Configuration des Mail Policies

Utilisation des Content Filters

- Présentation des Content Filters
- Conditions de filtrage du contenu
- Actions de filtrage de contenu
- Filtrer les messages en fonction du contenu
- Présentation 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

Utilisation des Content Filters pour appliquer des Mail Policies

- Présentation des filtres de messages
- Composants d'un filtre de messages
- Traitement du filtre des 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 de scan

Prévenir la perte de données

- Présentation du processus de scan DLP (Data Loss Prevention)
- Configuration du DLP
- Policies du DLP
- Actions relatives aux messages
- Mise à jour du moteur DLP et des classificateurs de correspondance de contenu

Utilisation de LDAP

- Présentation de LDAP
- Travailler avec LDAP
- Utilisation de 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 de récolte d'annuaire
- Requêtes de consolidation d'alias de quarantaine de spam

- Validation des destinataires à l'aide d'un serveur SMTP

Authentification de session SMTP

- Configuration d'AsyncOS pour l'authentification SMTP
- Authentification des sessions SMTP à l'aide de certificats clients
- Vérification de la validité d'un certificat client
- Authentification de l'utilisateur à l'aide de l'annuaire LDAP
- Authentification de la connexion SMTP via TLS à l'aide d'un certificat client
- Etablissement d'une connexion TLS à partir de l'Appliance
- Mise à jour d'une liste de certificats révoqués (CRL)

Authentification des Emails

- Présentation de l'authentification des emails
- Configuration de la signature DomainKeys et 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 des rapports et de la conformité de l'authentification des messages basée sur le domaine (DMARC)
- Détection des emails falsifiés

Cryptage des emails

- Vue d'ensemble de Cisco Email Encryption
- Chiffrement des messages
- Détermination des messages à chiffrer
- Insertion d'en-têtes de chiffrement dans les messages
- Cryptage des communications avec d'autres agents de transfert de messages (MTA)
- Travailler avec des certificats
- Gestion des listes d'autorités de certification
- Activation de TLS sur la Listener's Host Access Table (HAT)
- Activation de TLS et de la vérification des certificats à la livraison
- Services Secure/Multipurpose Internet Mail Extensions (S/MIME) Security

Utilisation des quarantaines système et des méthodes de livraison

- Décrire les quarantaines
- Quarantine de spam
- Configuration de la quarantaine de spam centralisée
- Utilisation de listes fiables et de listes de blocage pour contrôler la remise des e-mails en fonction de l'expéditeur
- Configuration des fonctionnalités de gestion du spam pour les utilisateurs finaux
- Gestion des messages dans la quarantaine de spam
- Quarantaine de policy, virus et d'outbreak
- Gestion des quarantaines de policy, de virus et outbreak
- Utilisation des messages dans les quarantaines de policy, de virus ou outbreak
- Modes de livraison

Gestion centralisée à l'aide de clusters

- Présentation de la gestion centralisée à l'aide de clusters
- Organisation du cluster
- Créer et rejoindre un cluster
- Gérer les clusters
- Communication du cluster
- Chargement d'une configuration dans des Appliance en cluster
- Les meilleures pratiques

Test et dépannage

- Débogage du flux de messagerie à l'aide de messages de test: trace
- Utilisation du listener pour tester l'Appliance
- Dépannage du réseau

- Dépannage du listener
- Dépannage de la remise des e-mails
- Dépannage des performances
- Problèmes d'apparence et de rendu de l'interface Web
- Répondre aux alertes
- Dépannage des problèmes matériels
- Travailler avec le support technique

Les références

- Spécifications du modèle pour les grandes entreprises
- Spécifications de modèle pour les entreprises de taille moyenne et les petites ou moyennes entreprises.
- Spécifications du Cisco Email Security Appliance virtuelles
- Licences

CERTIFICATION:

Cette formation prépare à l'examen Cisco 300-720 SESA