Securing the Web with Cisco Web Security Appliance (SWSA) v3.0
Cours officiel, préparation à l'examen 300-725 SWSA

Cours Pratique de 2 jours - 14h
Réf : JXE - Prix 2024 : 2 170€ HT

Avec cette formation "Sécuriser les accès Web avec Cisco Web Security Appliance", vous apprenez à mettre en œuvre, utiliser et entretenir l'appliance de sécurité Web Cisco® (WSA), optimisée par Cisco Talos. Ce matériel fournit une protection avancée de la messagerie professionnelle et permet le contrôle des menaces de sécurité web. Vous apprendrez également comment déployer des services proxy, comment utiliser l'authentification, mettre en œuvre des règles de contrôle du trafic et l'accès HTTPS, mettre en œuvre des paramètres et des stratégies de contrôle d'utilisation, et bien plus encore.

OBJECTIFS PÉDAGOGIQUES

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

Décrire Cisco Web Security Appliance (WSA)

Déployer des services proxy

Utiliser l'authentification

Décrire les politiques de déchiffrement pour contrôler le trafic HTTPS

Comprendre les politiques d'accès au trafic différenciées et les profils d'identification

Appliquer des paramètres de contrôle d'utilisation acceptables

Se défendre contre les logiciels malveillants

Décrire la sécurité des données et la prévention des pertes de données

Effectuer l'administration et le dépannage

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.

LE PROGRAMME

dernière mise à jour : 12/2021

1) Description de Cisco Web Security Appliance

- Cas d'utilisation de la technologie.
- Solution Cisco WSA.
- Fonctionnalités WSA.
- Architecture WSA.
- Service proxy.
- Moniteur de trafic de couche 4 intégré.
- Prévention de la perte de données.
- Intelligence cognitive Cisco.
- Outils de gestion.
- Rapports de sécurité Web avancés Cisco (AWSR) et intégration tierce.
- Appliance de gestion de la sécurité du contenu (SMA) de Cisco.

PARTICIPANTS

Architectes de sécurité, concepteurs de systèmes, administrateurs réseau, ingénieurs d'exploitation, gestionnaires de réseau, techniciens de réseau ou de sécurité, ingénieurs de sécurité, etc.

PRÉREQUIS

Avoir des connaissances sur TCP/IP, les services DNS, SSH, FTP, SNMP, HTTP et HTTPS. Avoir de l'expérience sur le routage IP. Être certifié CCNA. Connaissances de Windows.

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.

2) Déploiement des services proxy

- Mode de transfert explicite par rapport au mode transparent.
- Redirection du trafic en mode transparent.
- Protocole de contrôle du cache web.
- Flux en amont et en aval du protocole de communication de cache web (WCCP).
- Contournement de proxy.
- Mise en cache proxy.
- Fichiers de configuration automatique du proxy (PAC).
- Proxy FTP.
- Proxy Socket Secure (SOCKS).
- Journal d'accès proxy et en-têtes HTTP.
- Personnalisation des notifications d'erreur avec les pages de notification de l'utilisateur final (EUN).

3) Utilisation de l'authentification

- Protocoles d'authentification.
- Domaines d'authentification.
- Suivi des informations d'identification de l'utilisateur.
- Mode proxy explicite (forward) et transparent.
- Contournement de l'authentification avec des agents problématiques.
- Rapports et authentification.
- Ré-authentification.
- Authentification par proxy FTP.
- Dépannage de la jointure de domaines et test de l'authentification.
- Intégration avec Cisco Identity Services Engine (ISE).

4) Création de stratégies de déchiffrement pour contrôler le trafic HTTPS

- Présentation de l'inspection TLS (Transport Layer Security)/Secure Sockets Layer (SSL).
- Présentation du certificat.
- Présentation des politiques de déchiffrement HTTPS.
- Activation de la fonction proxy HTTPS.
- Balises de la liste de contrôle d'accès (ACL) pour l'inspection HTTPS.
- Exemples de journaux d'accès.

5) Stratégies d'accès au trafic différencié et les profils d'identification

- Présentation des stratégies d'accès.
- Groupes de stratégies d'accès.
- Présentation des profils d'identification.
- Profils d'identification et authentification.
- Ordre de traitement des politiques d'accès et des profils d'identification.
- Autres types de politiques.
- Exemples de journaux d'accès.
- Balises de décision ACL et groupes de stratégies.
- Application des politiques d'utilisation acceptables basées sur le temps et le volume de trafic.
- Notifications de l'utilisateur final.

6) Se défendre contre les logiciels malveillants

- Filtres de réputation de sites web.
- Analyse anti-malware.
- Analyse du trafic sortant.
- Anti-malware et réputation dans les politiques.
- Filtrage de la réputation des fichiers et analyse des fichiers.
- Protection avancée Cisco contre les logiciels malveillants.
- Fonctionnalités de réputation et d'analyse des fichiers.
- Intégration avec Cisco Cognitive Intelligence.

7) Application des paramètres de contrôle d'utilisation acceptables

- Contrôle de l'utilisation du web.
- Filtrage d'URL.
- Solutions de catégorie d'URL.
- Moteur d'analyse de contenu dynamique.
- Visibilité et contrôle des applications web.
- Application des limites de bande passante multimédia.
- Contrôle d'accès au logiciel en tant que service (SaaS).
- Filtrage du contenu réservé aux adultes.

8) Sécurité des données et prévention des pertes de données

- Sécurité des données.
- Solution de sécurité des données Cisco.
- Définitions de la politique de sécurité des données.
- Journaux de sécurité des données.

9) Exécution de l'administration et du dépannage

- Surveillance de l'appliance de sécurité web Cisco.
- Rapports Cisco Web Security Appliance (WSA).
- Surveillance de l'activité du système via les journaux.
- Tâches d'administration système.
- Dépannage.
- Interface de ligne de commande (CLI).

10) Références

- Comparaison des modèles WSA.
- Comparaison des modèles Cisco SMA.
- Présentation de la connexion, de l'installation et de la configuration.
- Déploiement du modèle OVF (Open Virtualization Format) de l'appliance de sécurité web Cisco.
- Mappage des ports de la machine virtuelle (VM) de l'appliance de sécurité web Cisco aux réseaux corrects.
- Connexion à l'appliance virtuelle de sécurité web Cisco.
- Activation du moniteur de trafic de couche 4 (L4TM).
- Accès et exécution de l'assistant de configuration du système.
- Reconnexion à l'appliance de sécurité web Cisco.
- Présentation de la haute disponibilité.
- Redondance matérielle.
- Présentation du protocole de redondance d'adresses communes (CARP).
- Configuration des groupes de basculement pour la haute disponibilité.
- Comparaison des fonctionnalités entre les options de redirection du trafic.
- Scénarios d'architecture lors du déploiement de Cisco AnyConnect® Secure Mobility.

11) Travaux pratiques officiels

- Configurer l'appliance de sécurité web Cisco.
- Déployer des services proxy.
- Configurer l'authentification proxy.
- Configurer l'inspection HTTPS.
- Créer et appliquer une politique d'utilisation acceptable basée sur l'heure/la date.
- Configurer la protection avancée contre les logiciels malveillants.
- Configurer les exceptions d'en-tête de référent.
- Utiliser des flux de sécurité tiers et un flux externe MS Office 365.
- Valider un certificat intermédiaire.
- Afficher les services de création de rapports et le suivi web.
- Effectuer une mise à niveau centralisée du logiciel Cisco AsyncOS à l'aide de Cisco SMA.

LES DATES

CLASSE À DISTANCE
2024 : 24 juin, 16 sept., 02 déc.