Formation : Securing the Web with Cisco Web Security Appliance (SWSA) v3.1

Cours officiel, préparation à l'examen 300-725 SWSA

Cours pratique - 2j - 14h00 - Réf. JXE
Prix : 2220 € H.T.

Avec cette formation, vous apprendrez à déployer, utiliser et administrer Cisco Web Security Appliance (WSA) pour protéger votre entreprise des menaces web. Vous configurerez des services proxy, l'authentification, des politiques de contrôle du trafic HTTPS, les fonctions anti-malware, la sécurité des données et la prévention des pertes d'informations, tout en assurant la gestion complète de la solution Cisco WSA.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Décrire Cisco WSA
- Déployer des services proxy
- Utiliser l'authentification
- Décrire les politiques de déchiffrement pour contrôler le trafic HTTPS
- Comprendre les politiques d'accès différenciées et les profils d'identification
- Appliquer les paramètres de contrôle d'usage acceptable
- Se défendre contre les malwares
- Décrire la sécurité des données et la prévention des pertes de données
- Effectuer l'administration et le dépannage

Public concerné

Architectes sécurité, concepteurs systèmes, administrateurs réseau, ingénieurs et managers sécurité, techniciens, intégrateurs et partenaires Cisco.

Prérequis

Connaissances des services TCP/IP (DNS, SSH, FTP, SNMP, HTTP/S), du routage IP, et compétences techniques de base (certif. Cisco, CompTIA, (ISC)², EC-Council, GIAC, ISACA ou équivalent).

PARTICIPANTS

Architectes sécurité, concepteurs systèmes, administrateurs réseau, ingénieurs et managers sécurité, techniciens, intégrateurs et partenaires Cisco.

PRÉREQUIS

Connaissances des services TCP/IP (DNS, SSH, FTP, SNMP, HTTP/S), du routage IP, et compétences techniques de base (certif. Cisco, CompTIA, (ISC)², EC-Council, GIAC, ISACA ou équivalent).

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 formation, 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.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

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

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.

Programme de la formation

1 Programme officiel

- Présentation de Cisco WSA.
- Déploiement des services proxy.
- Utilisation de l'authentification.
- Création de politiques de déchiffrement pour contrôler le trafic HTTPS.
- Compréhension des politiques d'accès différencié et des profils d'identification.
- Protection contre les malwares.
- Application des paramètres de contrôle d'usage acceptable.
- Sécurité des données et prévention des pertes de données.
- Administration et dépannage.
- Références.

2 Travaux pratiques officiels

- Configurer le Cisco Web Security Appliance.
- Déployer les services proxy.
- Configurer l'authentification proxy.
- Configurer l'inspection HTTPS.
- Créer et appliquer une politique d'usage acceptable basée sur l'heure et la date.
- Configurer la protection avancée contre les malwares.
- Configurer les exceptions d'en-tête référent.
- Utiliser des flux de sécurité tiers et le flux externe MS Office 365.
- Valider un certificat intermédiaire.
- Consulter les services de rapport et le suivi web.
- Effectuer une mise à jour centralisée du logiciel Cisco AsyncOS via Cisco SMA.

Options

Certification : 320 € HT

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.

Comment passer votre examen ?

L'option de certification se présente sous la forme d'un voucher ou d'une convocation qui vous permettra de passer l'examen à l'issue de la formation.

Dates et lieux

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.

CLASSE À DISTANCE
2026 : 30 juin, 15 déc.