Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS) v4.0

Cours officiel, préparation partielle à l'examen 300-710 SNCF

Cours Pratique de 5 jours
Réf : RJK - Prix 2022 : 4 260€ HT

Avec cette formation "Sécuriser les réseaux avec les IPS de dernière génération Cisco Firepower", vous apprenez à déployer et à utiliser le système de prévention des intrusions de nouvelle génération Cisco Firepower® (NGIPS). Vous abordez les fonctionnalités de la plateforme et les concepts de sécurité du pare-feu, l'architecture de la plateforme et les fonctionnalités clés. Vous voyez aussi l'analyse approfondie des événements, le réglage et la configuration du système de prévention des intrusions de nouvelle génération Cisco Firepower® (NGIPS), et bien plus encore.

PARTICIPANTS
Administrateurs de sécurité, conseillers en sécurité, administrateurs réseau, ingénieurs système, personnel de soutien technique, partenaires de distribution et revendeurs...

PRÉREQUIS
Compréhension technique des réseaux TCP/IP et de l'architecture réseau. Les bases des concepts des systèmes de détection d'intrusion (IDS) et des systèmes de prévention d'intrusion (IPS).

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.

OBJECTIFS PÉDAGOGIQUES

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

Décrire les composants de Cisco Firepower Threat Defense et le processus d'enregistrement des périphériques gérés

Détailler le contrôle du trafic des pare-feu de nouvelle génération (NFGW)

Configurer le système Cisco Firepower pour la découverte du réseau

Mettre en œuvre des politiques de contrôle d'accès

Décrire les fonctionnalités avancées de la politique de contrôle d'accès

Configurer les fonctionnalités d'intelligence de sécurité

Mettre en œuvre et gérer les politiques d'analyse d'intrusion et de réseau pour l'inspection NGIPS

Décrire les techniques d'analyse détaillées et les propriétés de rapport fournies par Cisco Firepower Management Center

Intégrer Cisco Firepower Management Center à une destination de journalisation externe

Décrire et démontrer les options d'alerte externes disponibles pour Cisco Firepower Management Center

Configurer une stratégie de corrélation

Décrire les principales fonctionnalités de mise à jour du logiciel Cisco Firepower Management Center

Décrire les principales fonctionnalités de gestion des comptes utilisateurs

Identifier les paramètres couramment mal configurés dans Cisco Firepower Management Center

Utiliser les commandes de base pour dépanner un périphérique Cisco Firepower Threat Defense

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) Programme officiel

- Présentation de Cisco Firepower Threat Defense.
- Configuration du périphérique Cisco Firepower NGFW.
- Contrôle du trafic Cisco Firepower NGFW.
- Découverte de Cisco Firepower.
- Implémentation des politiques de contrôle d'accès.
- Renseignement de sécurité.
- Contrôle des fichiers et protection avancée contre les logiciels malveillants (AMP).
- Systèmes de prévention des intrusions de nouvelle génération.
- Politiques d'analyse de réseau.
- Techniques d'analyse détaillées.

- Intégration de la plateforme Cisco Firepower.
- Politiques d'alerte et de corrélation.
- Exécution de l'administration du système.
- Dépannage de Cisco Firepower.

2) Travaux pratiques officiels

- Effectuer la configuration initiale de l'appareil.
- Effectuer la gestion des appareils.
- Configurer la découverte du réseau.
- Mettre en œuvre une politique de contrôle d'accès.
- Mettre en œuvre le renseignement de sécurité.
- Mettre en œuvre le contrôle et la protection avancée contre les logiciels malveillants.
- Mettre en œuvre NGIPS.
- Personnaliser une stratégie d'analyse de réseau.
- Effectuer une analyse.
- Configurer l'intégration de la plateforme Firepower avec Splunk.
- Configurer les alertes et la corrélation d'événements.
- Effectuer l'administration du système.
- Dépanner Firepower.

LES DATES

CLASSE A DISTANCE

2022 : 12 sept., 12 déc.