Security

Securing Networks with Cisco Firepower Next-Generation IPS

SSFIPS

Version : 4.0
5 Jours

Objectifs

A l'issue de ce cours, le stagiaire sera en mesure d'atteindre ses objectifs :

- Décrire les composants de Cisco Firepower Threat Defense et le processus d'enregistrement des périphériques gérés
- Détailler le trafic de pare-feu nouvelle génération (NGFW) et configurer le système Cisco Firepower pour la découverte du réseau
- Mettre en œuvre des politiques de contrôle d'accès et décrire les fonctionnalités avancées de la politique de contrôle d'accès
- Configurer les fonctionnalités d'intelligence de sécurité et la procédure de mise en œuvre de la protection avancée contre les logiciels malveillants (AMP) pour les réseaux pour le contrôle des fichiers et la protection avancée contre les logiciels malveillants
- Mettre en œuvre et gérer des politiques d'intrusion et d'analyse de réseau pour l'inspection NGIPS
- Décrire et démontrer les techniques d'analyse détaillées et les fonctionnalités de génération de rapports fournies par Cisco Firepower Management Center
- Intégrez Cisco Firepower Management Center à une destination de journalisation externe
- Décrire et démontrer les options d'alerte externes disponibles pour Cisco Firepower Management Center et configurer une stratégie de corrélation
- Décrire les principales fonctionnalités de mise à jour logicielle et de gestion des comptes d'utilisateurs de Cisco Firepower Management Center
- Identifiez les paramètres généralement mal configurés dans Cisco Firepower Management Center et utilisez les commandes de base pour dépanner un périphérique Cisco Firepower Threat Defense

Public Concerné

- Administrateurs de sécurité
- Consultants en sécurité
- Administrateurs réseau
- Ingénieurs système
- Personnel de support technique
- Partenaires et revendeurs

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

Pré-requis

Avant de suivre ce cours, le stagiaire doit posséder les compétences et les connaissances suivantes :

- Compréhension technique des réseaux TCP / IP et de l'architecture de réseau.
- Connaissance de base des concepts de systèmes de détection d'intrusion (IDS) et d'IPS.

Plan du cours détaillé

- Présentation de Cisco Firepower Threat Defense
- Configuration du périphérique Cisco Firepower NGFW
- Contrôle du trafic Cisco Firepower NGFW
- Cisco Firepower Discovery
- Implémentation de stratégies de contrôle d'accès
- Intelligence de sécurité
- Contrôle des fichiers et protection avancée contre les logiciels malveillants
- Systèmes de prévention des intrusions de nouvelle génération
- Stratégies d'analyse de réseau
- Techniques d'analyse détaillées
- Intégration de la plate-forme Cisco Firepower
- Politiques d'alerte et de corrélation
- L'administration du système
- Dépannage de Cisco Firepower

Laboratoire

- Configuration initiale de l'appareil
- Gestion d'appareils
- Configuration de la découverte du réseau
- Implémentation et politique de contrôle d'accès
- Implémentation de Security Intelligence
- Contrôle des fichiers et protection avancée contre les logiciels malveillants
- Implémentation de NGIPS
- Personnalisation d'une stratégie d'analyse de réseau
- Analyse détaillée
- Configuration de l'intégration de la plate-forme Cisco Firepower avec Splunk
- Configuration des alertes et de la corrélation d'événements
- L'administration du système
- Dépannage de Cisco Firepower

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00