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

Durée : 05 jours.

Ref : CI- SSFIPS

Course Overview

La formation vous montre comment déployer et utiliser le Cisco Firepower® Next-Generation Intrusion Prevention System (NGIPS). Ce cours pratique vous donne les connaissances et les compétences nécessaires pour utiliser les fonctionnalités de la plate-forme et inclut les concepts de sécurité de pare-feu, l'architecture de la plate-forme et les principales fonctionnalités ; l'analyse approfondie des événements, y compris la détection des logiciels malveillants et des types de fichiers sur le réseau, le réglage et la configuration du NGIPS, notamment le contrôle des applications, l'intelligence de sécurité, le pare-feu et les contrôles des logiciels malveillants et des fichiers sur le réseau ; le langage des règles Snort® ; l'inspection des fichiers et des logiciels malveillants, l'intelligence de sécurité et la configuration des politiques d'analyse du réseau conçues pour détecter les modèles de trafic ; la configuration et le déploiement des politiques de corrélation pour prendre des mesures en fonction des événements détectés ; le dépannage ; les tâches d'administration du système et des utilisateurs, et plus encore.

A qui s'adresse cette formation

Ce cours est conçu pour les professionnels techniques qui ont besoin de savoir comment déployer et gérer un Cisco Firepower NGIPS dans leur environnement réseau.

- Administrateurs sécurité
- Conseillers en sécurité

- Administrateurs réseau
- Ingénieurs système
- Personnel de soutien technique
- Partenaires de distribution et revendeurs

Certifications

Cette formation fait partie de la certification:

- Cisco Certified Network Professional Security (CCNP)

Pré-requis

Pour profiter pleinement de ce cours, vous devez posséder les connaissances et les compétences suivantes :

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

Objectifs

Ce cours vous aidera :

- Mettre en œuvre l'IPS Cisco Firepower Next-Generation pour arrêter les menaces, répondre aux attaques, augmenter la prévention des vulnérabilités contre les fichiers suspects et analyser les menaces pas encore identifiées.
- Acquérir des compétences de pointe pour des responsabilités très exigeantes axées sur la sécurité

Après avoir suivi ce cours, vous devriez être 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 Next-Generation (NGFW) et configurer le système Cisco Firepower pour la découverte du réseau
- Mettre en place des politiques de contrôle d'accès et décrire les fonctionnalités avancées de la politique de contrôle d'accès
- Configurer les fonctions 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 les politiques d'analyse d'intrusion et de réseau pour l'inspection du NGIPS
- Décrire et démontrer les techniques d'analyse détaillée et les fonctions de rapport fournies par le Cisco Firepower Management Center

- Intégrer le Cisco Firepower Management Center avec une destination de journalisation externe
- Décrire et démontrer les options d'alerte externe disponibles dans le Cisco Firepower Management Center et configurer une politique de corrélation
- Décrire les principales fonctionnalités de mise à jour du logiciel Cisco Firepower Management Center et de gestion des comptes utilisateurs
- Identifier les paramètres généralement mal configurés dans le Cisco Firepower Management Center et utiliser les commandes de base pour dépanner un dispositif Cisco Firepower Threat Defense

Contenu

- Aperçu de Cisco Firepower Threat Defense
- Configuration du dispositif Cisco Firepower NGFW
- Contrôle du trafic Cisco Firepower NGFW
- Découverte de Cisco Firepower
- Mise en œuvre des politiques de contrôle d'accès
- Renseignement de sécurité
- Contrôle des fichiers et protection avancée contre les logiciels malveillants
- Systèmes de prévention des intrusions de nouvelle génération
- Politiques d'analyse de réseau
- Techniques d'analyse détaillée
- Intégration de la plate-forme Cisco Firepower
- Politiques d'alerte et de corrélation
- Administration du système
- Dépannage de Cisco Firepower

Labs

- Configuration initiale de l'appareil
- Gestion des appareils
- Configuration de la découverte du réseau
- Politique de mise en œuvre et de contrôle d'accès
- Mise en œuvre du renseignement de sécurité
- Contrôle des fichiers et protection avancée contre les logiciels malveillants
- Mise en œuvre des NGIPS
- Personnalisation d'une politique d'analyse de réseau
- Analyse détaillée
- Configuration de l'intégration de la plate-forme Firepower de Cisco avec Splunk
- Configuration de l'alerte et de la corrélation des événements
- Administration du système
- Dépannage de la puissance de feu Cisco