

Securing Networks with Cisco Firepower Next-Generation IPS

Description

Cette formation vous apprend comment déployer et utiliser le Cisco Firepower® Next-Generation Intrusion Prevention System (NGIPS). Elle 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.

Contenu du cours

- 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

Lab / Exercices

Laboratoires officiels CISCO :

- 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

Documentation

- Support de cours numérique officiel CISCO

Examen

- Ce cours vous prépare à la certification "Securing Networks with Cisco Firepower (300-710 SNCF)" qui conduit aux certifications "CCNP Security et Cisco Certified Specialist - Network Security Firepower". L'examen 300-710 SNCF a également un deuxième cours de préparation "Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)". Vous pouvez suivre ces cours dans n'importe quel ordre.

Profils des participants

- 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

Connaissances Préalables

- 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

- 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

Niveau

Avancé

Prix de l'inscription en Présentiel (CHF)

4600

Prix de l'inscription en Virtuel (CHF)

4350

Durée (Nombre de Jours)

5

Reference

CIS-SSFIPS