Formation Cisco Security : Maîtriser la sécurisation des réseaux avec Cisco Firepower Next Generation

Description de la formation Cisco Firepower Next Generation

Cette formation Cisco Firepower Next Generation est composée des modules Le module Sécuriser les réseaux avec Cisco Firepower Next Generation IPS et Le module Sécuriser les réseaux avec Cisco Firepower Next Generation Firewall

Le module Sécuriser les réseaux avec Cisco Firepower Next Generation IPS vous apprend à déployer et à utiliser le Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS).

Il vous donne tous les outils 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, le réglage et la configuration du NGIPS, l'intelligence de sécurité, le langage des règles Snort, l'inspection des fichiers et des logiciels malveillants, 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.

Le module Sécuriser les réseaux avec Cisco Firepower Next Generation Firewall vous montre comment déployer et utiliser le système de défense Cisco Firepower Threat Defense.

Vous apprendrez à mettre en œuvre les fonctionnalités avancées du pare-feu de nouvelle génération (NGFW) et du système de prévention des intrusions de nouvelle génération (NGIPS), notamment l'intelligence réseau, la détection des types de fichiers, la détection des logiciels malveillants sur le réseau et l'inspection approfondie des paquets. Vous verrez

également comment configurer le VPN de site à site, le VPN d'accès à distance et le décryptage SSL avant de passer à l'analyse détaillée, à l'administration système et au dépannage.

Objectifs

À l'issue de cette **formation Cisco Firepower Next Generation**, vous aurez acquis les connaissances et compétences nécessaires pour :

- 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
- Décrire les concepts clés des technologies NGIPS et NGFW et du système de défense contre les menaces Cisco Firepower, et identifier les scénarios de déploiement

- Effectuer les tâches initiales de configuration et d'installation des dispositifs de défense contre les menaces de Cisco Firepower
- Décrire comment gérer le trafic et mettre en œuvre la qualité de service (QoS) en utilisant Cisco Firepower Threat Defense
- Décrire comment mettre en œuvre la NAT en utilisant Cisco Firepower Threat Defense
- Effectuer une découverte initiale du réseau, en utilisant Cisco Firepower pour identifier les hôtes, les applications et les services
- Décrire le comportement, l'utilisation et la procédure de mise en œuvre des politiques de contrôle d'accès
- Décrire les concepts et les procédures de mise en œuvre des caractéristiques du renseignement de sécurité

À qui s'adresse cette formation ?

Public :

Ce cours Cisco Firepower Next Generation s'adresse principalement aux administrateurs de sécurité, consultants en sécurité, administrateurs réseau, ingénieurs système, personnels de support technique, partenaires et revendeurs.

Prérequis :

Pour suivre cette formation Cisco Firepower Next Generation, les participants doivent avoir une compréhension technique des réseaux TCP/IP et de l'architecture des réseaux, ainsi qu'une connaissance de base des concepts de systèmes de détection d'intrusion (IDS), d'IPS et des pare-feux.

Contenu du cours Cisco Firepower Next Generation

Module 1 : Sécuriser les réseaux avec Cisco Firepower Next Generation IPS

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

Module 2 : Sécuriser les réseaux avec Cisco Firepower Next Generation Firewall

Présentation de Cisco Firepower Threat Defense

Examen de la technologie des pare-feu et IPS
Caractéristiques et composants de Firepower Threat Defense
Examen des plates-formes de Firepower
Cas d'utilisation de la mise en œuvre de Cisco Firepower

Configuration du dispositif Cisco Firepower Next Generation Firewall

Enregistrement des dispositifs à Firepower Threat Defense
FXOS et Firepower Device Manager

Configuration initiale de l'appareil

Gestion des dispositifs de NGFW

Examen des politiques du Centre de gestion de Firepower

Examen des objets

Examen de la configuration du système et de la surveillance de la santé

Gestion des appareils

Examen de la haute disponibilité de Firepower

Configuration de la haute disponibilité

Migration de Cisco ASA vers Firepower

Migration de Cisco ASA vers Firepower Threat Defense

Contrôle du trafic de Cisco Firepower Next Generation Firewall

Traitement des paquets de Firepower Threat Defense

Mise en œuvre de la QoS

Contournement de la circulation

Traduction d'adresses Cisco Firepower Next Generation Firewall

Principes de base du NAT

Implémentation de NAT

Exemples de règles NAT

Implémentation de NAT

Découverte de Cisco Firepower (Cisco Firepower Discovery)

Examen de la découverte du réseau

Configuration de la découverte du réseau

Mise en œuvre des politiques de contrôle d'accès

Examen des politiques de contrôle d'accès

Examen des règles de la politique de contrôle d'accès et des mesures par défaut

Mise en œuvre d'une inspection plus poussée

Examen des événements de connexion

Politique de contrôle d'accès Paramètres avancés

Considérations relatives à la politique de contrôle d'accès

Mise en œuvre d'une politique de contrôle d'accès

Security Intelligence

Examen de Security Intelligence

Examen des objets de Security Intelligence

Déploiement et enregistrement de Security Intelligence

Mise en œuvre de Security Intelligence

Contrôle des fichiers et protection avancée contre les logiciels malveillants

Examen des logiciels malveillants et de la politique des fichiers

Examen de la protection avancée contre les logiciels malveillants

Systèmes Next Generation de prévention des intrusions

Examen de la prévention des intrusions et des règles de Snort

Examen des variables et des ensembles de variables

Examen des politiques d'intrusion

VPN de site à site

Examen d'IPsec

Configuration VPN de site à site

Dépannage VPN de site à site

Mise en place d'un VPN de site à site

VPN d'accès à distance

Examen du VPN d'accès à distance

Examen de la cryptographie à clé publique et des certificats

Inscription au certificat d'examen

Configuration du VPN d'accès à distance

Mise en œuvre d'un VPN d'accès à distance

Décryptage SSL

Examen du décryptage SSL
Configuration des politiques SSL
Best Practices et surveillance du décryptage SSL

Techniques d'analyse détaillée

Examen de l'analyse des événements
Examen des types d'événements
Examen des données contextuelles
Examen des outils d'analyse
Analyse de la menace

Administration du système

Gestion des mises à jour
Examen des caractéristiques de la gestion des comptes utilisateurs
Configuration des comptes d'utilisateur
Administration du système

Dépannage de Cisco Firepower

Examen des erreurs de configuration courantes
Examen des commandes de dépannage
Dépannage de Firepower

Travaux Pratiques

De nombreux travaux pratiques seront proposés aux participants tout au long des dix journées de formation. Ces travaux pratiques concernent notamment :

- 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
- Configuration initiale de l'appareil
- Gestion d'appareils
- Configuration de la haute disponibilité
- Migration de Cisco ASA vers Cisco Firepower Threat Defense
- Implémentation de la QoS
- Implémentation de NAT
- Configuration de la découverte du réseau
- Implémentation d'une politique de contrôle d'accès
- Implémentation de Security Intelligence
- Implémentation d'un VPN de site à site
- Implémentation d'un VPN d'accès à distance
- Analyse des menaces
- L'administration du système
- Dépannage de la puissance de feu