CISCO

Sécuriser les réseaux avec les firewalls de dernière génération Cisco Firepower (SSNGFW)

5 jours (35h00) | CIS012 | Num form : form-165 | Perfectionnement / Avancé

INFORMATIQUE / INFRASTRUCTURE / CISCO

À l'issue de ce stage vous serez capable de :

- 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 oeuvre la qualité de service (QoS) en utilisant Cisco Firepower Threat Defense
- Décrire comment mettre en oeuvre 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 oeuvre des politiques de contrôle d'accès
- Décrire les concepts et les procédures de mise en oeuvre des caractéristiques du renseignement de sécurité
- Se préparer à l'examen Securing Networks with Cisco Firepower (300-710 SNCF)

Niveau requis :

- Compréhension technique de la mise en réseau TCP/IP et de l'architecture réseau
- Connaissance de base des concepts de pare-feu et d'IPS

Public concerné :

- Administrateurs de la sécurité
- Conseillers en sécurité
- Administrateurs réseau

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

Programme :

APERÇU DE CISCO FIREPOWER THREAT DEFENSE

- Examen de la technologie des pares-feux et IPS
- Caractéristiques et composants de Firepower Threat Defense
- Examen des plates-formes de Firepower
- Cas d'utilisation de la mise en oeuvre de Cisco Firepower

CONFIGURATION DU DISPOSITIF CISCO FIREPOWER NGFW

- 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 NGFW

- Traitement des paquets de Firepower Threat Defense
- Mise en oeuvre de la QoS
- Contournement de la circulation

TRADUCTION D'ADRESSES CISCO FIREPOWER NGFW

- 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 oeuvre 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 oeuvre 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 oeuvre 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 oeuvre 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 oeuvre 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