Développez vos talents
Certifiez vos compétences

Cisco - Offre officielle certifiante

Securing Networks with Cisco Firepower Next-Generation IPS

5 jours (35h00) | ★★★★½ 4,6/5 | SSFIPS | Certification 300-710 (non incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Réseaux et Télécoms › Cisco - Offre officielle certifiante

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

- Mettre en oeuvre 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
- Mettre en oeuvre des compétences de pointe pour des responsabilités très exigeantes axées sur la sécurité
- Décrire les composants de Cisco Firepower Threat Defense et le processus d'enregistrement des périphériques gérés
- Détailler le contrôle du trafic Next-Generation Firewalls (NGFW) et configurer le système Cisco Firepower pour la découverte du réseau
- Mettre en place des politiques de contrôle d'accès et identifier leurs fonctionnalités avancées
- Configurer les fonctions de Security Intelligence et la procédure de mise en oeuvre d'Advanced Malware Protection (AMP) pour les réseaux afin d'assurer le contrôle des fichiers et la protection avancée contre les logiciels malveillants
- Mettre en oeuvre et gérer les politiques d'analyse d'intrusion et de réseau pour l'inspection du Next-Generation Intrusion Prevention System (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
- Expliquer 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.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Niveau requis

Avoir des connaissances de base sur les systèmes de détection d'intrusion (IDS) et IPS, et des connaissances techniques sur les réseaux TCP/IP et sur l'architecture des réseaux. De plus, il est recommandé d'avoir suivi les cours CCNA "Cisco Solutions - Implementing and administering" et SCOR "Cisco Security Core Technologies - Implementing and operating", ou avoir les connaissances équivalentes. Afin d'obtenir la certification CCNP Security, il faut avoir passé l'examen Core 350-701 et l'examen 300-710.

Public concerné

Administrateurs sécurité, conseillers en sécurité, administrateurs réseau, ingénieurs système, personnel de soutien technique, partenaires de distribution et revendeurs et/ou professionnels techniques souhaitant savoir déployer et gérer un Cisco Firepower NGIPS dans leur environnement réseau.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Aperçu de Cisco Firepower Threat Defense

Configuration du dispositif Cisco Firepower NGFW

Contrôle du trafic Cisco Firepower NGFW

Découverte de Cisco Firepower

Mise en oeuvre des politiques de contrôle d'accès

Security Intelligence

Contrôle des fichiers et protection avancée contre les logiciels malveillants

Next-Generation Intrusion Prevention Systems

Politiques d'analyse de réseau

Techniques d'analyse détaillée

Intégration de la plateforme 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 oeuvre et de contrôle d'accès*
- *Mise en oeuvre de Security Intelligence*
- *Contrôle des fichiers et protection avancée contre les logiciels malveillants*
- *Mise en oeuvre de NGIPS*
- *Personnalisation d'une politique d'analyse de réseau*
- *Analyse détaillée*
- *Configuration de l'intégration de la plateforme Firepower de Cisco avec Splunk*
- *Configuration de l'alerte et de la corrélation des événements*
- *Administration du système*
- *Dépannage de Cisco Firepower*

Certification (en option)

- Prévoir l'achat de la certification en supplément
- Le passage de l'examen se fera (ultérieurement) dans un centre agréé Pearson Vue
- L'examen (en anglais) s'effectue en ligne, et durera en moyenne 1h30

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)

Les + de la formation

Le support de cours et les labs sont en anglais.