Formation Sécuriser les réseaux avec Cisco Firepower Next-Generation IPS

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

La formation Sécurisation des réseaux avec Cisco Firepower Next-Generation IPS explique et démontre comment déployer et utiliser les Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS). Ce cours, avec des exercices pratiques, vous donne les connaissances et les compétences requises pour utiliser les fonctionnalités de la plateforme, en incluant les concepts de sécurité du pare-feu, connaitre l'architecture de la plateforme et les fonctions clés; analyser de manière approfondie des événements, y compris la détection des logiciels malveillants et des types de fichier sur le réseau, configurer et optimiser NGIPS, incluant le contrôle des applications, les renseignements de sécurité, le pare-feu et la détection des logiciels malveillants, ainsi que les contrôles de fichiers, basés sur le réseau, connaitre les règles du langage Snort; configurer des politiques pour l'inspection des fichiers et des logiciels malveillants, pour les renseignements de sécurité et pour l'analyse du réseau conçues pour détecter des types de trafic ; configurer et déployer des politiques de corrélation pour prendre des mesures en fonction des événements détectés; dépanner; administrer le système et les utilisateurs, et plus encore.
Le suivi de cette formation permet de valider un total de 32 crédits dans le cadre du programme d'Education Continue Cisco (CCE) pour les professionnels qui souhaitent renouveler leur titre de certification.

Référence	SSFIPS
Durée	5 jours (35h)
Tarif	4 290 €HT
Repas	100 €HT(en option)

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 18 au 22 novembre 2024

VOIR TOUTES LES DATES

Objectifs

| Décrire les composants de Cisco Firepower Threat Defense et le processus d'enregistrement de périphérique géré
| Détailler le contrôle du trafic par Next-Generation Firewalls (NGFW) et configurer le système Cisco Firepower system pour la découverte du réseau
| Mettre en oeuvre des politiques de contrôle d'accès et décrire les fonctionnalités avancées de la politique de contrôle d'accès
| Configurer les fonctionnalités d'intelligence de sécurité et la mise en oeuvre des procédures de contrôle des fichiers et de protection avancée contre les logiciels malveillants (AMP Advanced Malware Protection)
| Mettre en oeuvre et gérer des poltiiques d'intrusion et d'analyse de réseau pour l'inspection NGIPS
| Décrire et démontrer les options d'alertes externes disponibles de Cisco Firepower Management Center et configurer des politiques de corrélations
| Intégrer Cisco Firepower Management Center à un serveur externe de rapports
| Décrire et démontrer les options d'alerte externes disponbiles pour Cisco FirePower Management Center et configurer une politique de corrélation
| Décrire les fonctions clés pour la mise à jour logicielle de Cisco FirePower Management Center et la gestion des comptes utilisateurs
| Identifier les paramètres généralement mal configurés dans Cisco FirePower Management Center et utiliser les commandes de base pour dépanner un dispositif FirePower Threat Defense

Public

| Techniciens professionnels qui ont besoin de savoir comment déployer et gérer un Cisco FirePower NGIPS dans leur environnement réseau

Prérequis

| Compréhension technique des réseaux TCP / IP et de l'architecture de réseau

| Connaissance de base des concepts de système de détection d'intrusion (IDS) et IPS
| CCNA Security (CCNA and IINS) recommandé.

Programme de la formation

Présentation Cisco Firepower Threat Defense
Security Intelligence
Intégarion de la plateforme Cisco Firepower
Configuration du dispositif Cisco Firepower NGFW
Contrôle des fichiers et protection avancée contre les logiciels malveillants
Politiques d'alerte et de corrélation
Contrôle de trafic Cisco Firepower NGFW
Découverte du réseau par Cisco Firepower
Système NGIPS (Next-Generation Intrusion Prevention Systems)
L'administration du système
Dépannage de Cisco Firepower
Implémentation des politiques de contrôle d'accès
Stratégies d'analyse de réseau
Travaux pratiques:
| Techniques d'analyse détaillées
| Configuration initiale de l'équipement
| Management de l'équipement
| Configurer les politiques de découverte réseau
| Politique de mise en oeuvre et de contrôle d'accès
| Mise en oeuvre de l'intelligence de sécurité
| Contrôle des fichiers et protection avancée contre les logiciels malveillants
| Mise en oeuvre de NGIPS
| Personnalisation d'une stratégie d'analyse de réseau
| Analyse détaillée
| Configurer l'intégration de Cisco Firepower Platform Integration avec Splunk
| Configuration des alertes et de la corrélation des événements
| Administration du système
| Dépannage de Cisco Firepower

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.