FIREPOWER: SECURING NETWORKS WITH CISCO FIREPOWER THREAT DEFENSE

CODE DE LA FORMATION:
CS-SC-FIREPOWER

ÉDITEUR OU CONSTRUCTEUR:
CISCO

DURÉE:
5 JOURS

Ce cours permettra aux ingénieurs travaillant dans le domaine de la sécurité d'apprendre les différentes fonctionnalités avancées de Cisco Firepower Threat Defense incluant la configuration du NAT, le control du trafic avec les Access Control Policies, la qualité de service, SSL Decryption, la configuration du VPN, la configuration avancee de AMP, contrôle de fichier et NGIPS, le Network Discovery ainsi que l'analyse des événements au niveau de Firepower Management center et le dépannage.

Ce cours vous initiera à configurer les différentes composantes du Firepower Threat Defense en commençant par la configuration basique comme les adresses IP, le routage, la translation des adresses ainsi que les access control policies, ensuite il permettra aux participants l'implémentation avancée du FTD comme le système de prévention nouvelle génération (NGIPS) et les bonnes pratiques, le Network Discovery pour identifier les hôtes, les applications, les services et les vulnérabilités, particulièrement comment exploiter ses vulnérabilités afin de configurer une Policy IPS appropriée et adaptée a votre réseau à l'aide de la fonction Firepower Recommendation, l'AMP pour protéger votre réseau des menaces malwares, security intelligence pour agir rapidement contre les menaces provenant de l'extérieur en utilisant security intelligence ainsi que les filtrage du type de fichier.

Aussi les participants apprendront comment configurer un VPN Site to Site, le VPN Remote Access et SSL Decryption pour inspecter le trafic crypté, enfin l'analyse détaillée des évènements collectes par la console de management Firepower Management Center et le dépannage.

PRÉREQUIS:

Avant de suivre cette formation, le participant doit posséder les connaissances suivantes

- Connaissances en TCP/IP.
- Connaissances basiques en Firewalling et IPS

PUBLIC:

- Administrateurs sécurité
- Consultant en sécurité
- Administrateur réseau

OBJECTIFS:

A l'issue de la formation, les stagiaires seront en mesure de :

- Comprendre les différents composants du Firepower Threat Defense.
- Intégrer le Firepower Threat Defense dans la console de management FMC.
- Configurer les adresses IP et le routage pour la connectivité, le NAT et la QoS.
- Configurer le network discovery pour identifier les hôtes, les applications, les services et les vulnérabilités.
- Comprendre la logique et la configuration des access control policies.
- Apprendre a configurer la fonctionnalité security intelligence
- Configurer AMP pour l'analyse dynamique au niveau cloud et l'analyse locale des fichiers ainsi que le control de ses fichiers par type.
- Implémenter et optimiser le système de prévention d'intrusion avec firepower recommendation.
- Comprendre les étapes de fonctionnement des VPNs site to site et remote access ainsi que l'implémentation.
- Comprendre les différentes méthodes pour mettre en place une policy de SSL Decryption.
- Apprendre à exploiter les évènements collectes par la FMC pour l'analyse du trafic et leur trajectoire

CONTENU:

- Module 1: Cisco Firepower Defense Overview
- Module 2: Cisco Firepower Setup
- Module 3: QoS and NAT Implementation
- Module 4 : Cisco Firepower Discovery
- Module 5: Access Control Policy Prerequisites
- Module 6: Implementing Access Control Policies
- Module 7: Security Intelligence
- Module 8: AMP for Networks Malware Protection
- Module 9: Next-Generation Intrusion Prevention Systems
- Module 10: VPN Site-to-Site
- Module 11: Remote Access VPN
- Module 12: SSL Decryption
- Module 13: Detailed Analysis Techniques
- Module 14: System Administration
- Module 15: Cisco Firepower Threat Defense Troubleshooting