FORMATION PALO ALTO NETWORKS FIREWALL 10.1 – CONFIGURATION & MANAGEMENT

INFORMATIONS GÉNÉRALES

Domaine : Cybersécurité - sécurité informatique

Filière : Sécurité défensive

Rubrique : SOC (Security Operations Center)

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

- Configurer et gérer les fonctionnalités essentielles des firewalls Palo Alto Networks de nouvelles générations
- Configurer et gérer des règles de sécurités et de NAT pour la gestion des flux autorisés
- Configurer et gérer les profils de gestion des menaces afin de bloquer les trafics provenant des adresses, domaines et URLs connues et inconnues
- Monitorer le trafic réseau en utilisant l'interfaces web et les rapports intégrés

Public visé

Ingénieur sécurité
Administrateurs sécurité
Analystes en sécurité
Ingénieurs réseaux
Membres d'une équipe de support

Pré-requis

Les participants devront être familiers avec les concepts basics de la sécurité et des réseaux, incluant routage, switching et adresses IP.
Une expérience sur des technologies de sécurité (IPS, proxy, filtrage de contenus) est un plus

PROGRAMME

Palo Alto Networks portfolio et architecture
Configuration initiale du Firewall
Gérer les configurations sur le Firewall
Gérer les comptes d'administration du Firewall
Connection du Firewall aux réseaux de production avec zones de sécurités
Création et gestion des règles de sécurité
Création et gestion des règles de NAT
Contrôle des applications avec App-ID
Blocages des menaces connues en utilisant les profils de sécurité
Blocage du trafic web non approprié avec le filtrage des URLs
Bloquer les menaces inconnues avec Wildfire
Contrôler l'accès aux ressources réseaux avec la reconnaissance utilisateurs (User-ID)
Utiliser le déchiffrement afin de bloquer les menaces sur un trafic chiffré
Repérer les informations importantes via les logs et les rapports
Discussion sur les autres formations et les certifications
Annexe A - Sécuriser les postes de travail avec Global Protect
Annexe B - Apporter de la redondance au Firewall avec la haute disponibilité
Annexe C - Connecter des sites distants via des VPN site à site
Annexe D - Configuration de l'agent Windows User-ID

Code de formation : SP77883

€ Tarifs

Lieux & Horaires

Campus : Ensemble des sites

Durée : 35 heures

Délai d'accès :
Jusqu'à 8 jours avant le début de la formation

Distanciel possible : Oui

Prochaines sessions

Cliquez sur la date choisie pour vous inscrire :

- 07 / 10 / 2024
: Ensemble des sites
: Distanciel possible
: 35 heures
: 5 jours

MODALITÉS

Méthode

Fin de formation : entretien individuel
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation
Assiduité : certificat de réalisation (validation des acquis)