FORMATION PALO ALTO NETWORKS FIREWALL 10.1 – CONFIGURATION & MANAGEMENT

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

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

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 35 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.