DAWAN

Plan de la formation

www.dawan.fr

Formation CheckPoint R81.X Security Intermédiaire

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	2 375,00 CHF HT (standard) 1 900,00 CHF HT (remisé)
Public :	Administrateurs réseaux, techniciens IT
Pré-requis :	Utiliser couramment CheckPoint R81.X
Objectifs :	Comprendre les concepts de CheckPoint R81.X. Configurer et gérer des dispositifs de sécurité. Surveiller et analyser le trafic réseau. Déployer des politiques de sécurité avancées. Effectuer des diagnostics et résoudre les problèmes courants.
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	RéS102299-F
Note de satisfaction des participants:	4,70 / 5
Contacts :	commercial@dawan.fr - 09 72 37 73 73

Modalités d’accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Introduction à Check Point R81.X

Check Point et les versions R81.X.
Découvrir l’architecture de la solution Check Point.
Identifier les composants de la passerelle de sécurité.
Atelier : Exploration des composants de la passerelle de sécurité.

Configuration avancée des politiques de sécurité

Créer des règles de sécurité avancées.
Gérer les objets et les groupes.
Implémenter des politiques de sécurité basées sur les utilisateurs.
Utiliser les applications et les contrôles de contenu.
Atelier : Création et gestion des règles de sécurité avancées.

Gestion du trafic réseau

Configurer les VPN (Site à Site et Remote Access).
Configurer les tunnels IPsec.
Gérer les connexions et le routage.
Atelier : Configuration des VPN et des tunnels IPsec.

Surveillance et analyse

Utiliser les outils de surveillance intégrés.
Analyser les journaux et les rapports.
Configurer SmartView Tracker et SmartLog.
Détecter et répondre aux incidents.
Atelier : Utilisation des outils de surveillance et analyse des journaux.

Diagnostic et résolution des problèmes

Utiliser les outils de diagnostic (cpstat, fw monitor, etc.).
Résoudre les problèmes courants.
Appliquer les meilleures pratiques pour la maintenance et l’administration.
Atelier : Diagnostic et résolution des problèmes courants.

Études de cas et exercices pratiques

Mettre en pratique les connaissances acquises à travers des scénarios réalistes.
Discuter en groupe des défis rencontrés.
Résoudre des problèmes en temps réel.
Atelier : Études de cas et résolution de problèmes en temps réel.