DAWAN

Plan de la formation

www.dawan.fr

Formation CheckPoint R81.X Security Avancé

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 :	Avoir suivi la formation CheckPoint R81.X Security Intermédiaire ou posséder les connaissances équivalentes.
Objectifs :	Mettre en œuvre des configurations de sécurité avancées. Gérer des menaces avancées et des attaques ciblées. Configurer et optimiser les fonctionnalités de prévention des menaces. Intégrer Check Point avec des solutions tierces pour une sécurité renforcée. Effectuer des audits de sécurité et des évaluations de conformité.
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 :	RéS102300-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

Concepts de sécurité avancés

Comprendre les menaces modernes et les attaques avancées.
Analyser les techniques d’attaque (phishing, ransomware, etc.).
Expliquer les modèles de menace et la gestion des risques.
Atelier : Analyse des techniques d’attaque avancées.

Prévention des menaces

Configurer et optimiser Threat Prevention (Antivirus, Anti-Bot, IPS).
Utiliser SandBlast pour la protection contre les menaces avancées.
Appliquer les meilleures pratiques pour la configuration de la prévention des menaces.
Atelier : Configuration et optimisation de Threat Prevention.

Sécurisation des environnements Cloud et virtuels

Configurer la sécurité pour les environnements virtuels (VMware, Azure, etc.).
Intégrer Check Point avec des solutions Cloud.
Gérer les politiques de sécurité dans des environnements hybrides.
Atelier : Configuration de la sécurité pour les environnements virtuels.

Intégration des solutions tierces

Intégrer Check Point avec des solutions SIEM (Security Information and Event Management).
Utiliser les API Check Point pour l’automatisation de la sécurité.
Mettre en place l’interopérabilité avec d’autres dispositifs de sécurité.
Atelier : Intégration de Check Point avec des solutions SIEM.

Audit et conformité de la sécurité

Utiliser les outils et méthodologies pour l’audit de sécurité.
Vérifier la conformité avec les réglementations (GDPR, PCI-DSS, etc.).
Générer des rapports de sécurité et des recommandations d’amélioration.
Atelier : Vérification de la conformité et génération de rapports de sécurité.

Études de cas et scénarios pratiques

Étudier des cas réels d’incidents de sécurité.
Simuler des scénarios pratiques de réponse aux incidents.
Analyser la réponse à des attaques simulées.
Atelier : Études de cas et simulation d’attaques.