DAWAN

Plan de la formation

www.dawan.fr

Formation CheckPoint EndPoint Security : Fondamentaux

Durée :	2 jours (14 heures)
Tarifs inter-entreprise :	1 575,00 CHF HT (standard) 1 260,00 CHF HT (remisé)
Public :	Administrateurs réseaux, techniciens IT
Pré-requis :	Avoir des connaissances de base en réseaux, sécurité informatique, et familiarité avec les environnements Windows et Linux.
Objectifs :	Permettre aux participants de maîtriser l'installation, la configuration, la gestion et le dépannage de la solution CheckPoint Endpoint Security pour protéger efficacement les points d'extrémité au sein d'une infrastructure réseau.
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 :	CYB102295-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 CheckPoint Endpoint Security

Aperçu de Endpoint Security.
Vue d'ensemble des solutions CheckPoint.
Enjeux de la sécurité des points d'extrémité.
Présentation CheckPoint Endpoint Security et Secure Access R71.
Identifier les concepts clés : VPN, Firewall, Anti-Malware, Data Protection, etc.
Découvrir l'interface de gestion CheckPoint SmartConsole.
Atelier : Exploration de l'interface d'administration et des fonctionnalités de base.

Architecture et Composants de CheckPoint R71

Identifier les composants principaux : Endpoint Security Client, Management Server.
Expliquer le fonctionnement des modules (Secure Access, VPN, Device Control).
Comprendre la communication entre les composants et la gestion des policies.
Analyser le flux de données et de communication entre les composants.
Atelier : Diagramme d'architecture d'une infrastructure Checkpoint R71.

Installation de CheckPoint Endpoint Security

Définir les prérequis matériels et logiciels.
Installer le Management Server.
Installer et configurer l'EndPoint Client.
Dépanner les problèmes courants lors de l'installation.
Effectuer une installation pas à pas sur un environnement de test.
Atelier : Installation des composants dans un environnement virtuel ou sur des machines locales.

Configuration des politiques de sécurité de base

Introduire la gestion des policies de sécurité.
Créer des politiques de base : Règles de Firewall, contrôle des applications, accès VPN.
Gérer les utilisateurs et les groupes.
Développer des stratégies de déploiement des policies.
Configurer les règles via SmartDashboard.
Atelier : Création de politique de sécurité et leur application sur les endpoints.

Gestion des accès VPN et sécurisation des communications

Introduire le VPN SSL et POSec.
Configurer les accès VPN pour les utilisateurs distants.
Mettre en œuvre les certificats et l'authentification.
Configurer des paramètres avancés : Split tunneling, contrôle d'accès dynamique.
Mettre en place un VPN SSL/IPSec pour les utilisateurs distants.
Atelier : Configuration et test d'une connexion VPN sécurisé.

Protection des données et gestion des menaces

Configurer les modules Anti-Malware et Anti-Phishing.
Surveiller les données sensibles et gérer les fuites de données (Data Loss Prevention).
Analyser les menaces et répondre aux incidents.
Mettre à jour les signatures et configurer des alertes.
Configurer le module Anti-Malware et Data Loss Prevention.
Atelier : Détection et blocage d'une tentative d'infection par malware.

Gestion et déploiement à grande échelle

Centraliser la gestion des points d'extrémité.
Déployer automatiquement le client Endpoint.
Gérer les mises à jour logicielles et les correctifs.
Surveiller les points d'extrémité : logs, rapports, tableaux de bord.
Déployer en masse via les outils CheckPoint.
Atelier : Surveillance et gestion des mises à jour dans une infrastructure test.

Maintenance et Dépannage

Surveiller et gérer les performances des clients.
Analyser les journaux et les diagnostics pour identifier les problèmes.
Résoudre les problèmes de connexion VPN, de performance ou de politiques de sécurité.

Supporter les utilisateurs finaux et dépanner à distance.
Utiliser les outils de diagnostics CheckPoint.
Atelier : Simulation de divers scénarios de panne et résolution.