

Formation : Check Point R81, sécurité réseaux, niveau 1

Cours pratique - 4j - 28h00 - Réf. CPB

Prix : 2960 CHF H.T.

Ce cours vous fera découvrir la dernière version des produits Check Point : R81.20. A l'issue de cette formation, vous serez capable de mettre en place et gérer une politique de sécurité unifiée (Access Control et Threat Prevention) ainsi que des politiques de sécurité partagées (Geo Policy et HTTPS Inspection).

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Installer et configurer Check Point R81
- Mettre en œuvre une politique de sécurité
- Mettre en œuvre l'examen et le filtrage des logs
- Bloquer les intrusions avec SAM (Suspicious Activity Monitor)

Public concerné

Administrateurs et ingénieurs systèmes/réseaux/sécurité, techniciens.

Prérequis

Bonnes connaissances de TCP/IP. Connaissances de base en sécurité informatique.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant [ce test](#).

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

PARTICIPANTS

Administrateurs et ingénieurs systèmes/réseaux/sécurité, techniciens.

PRÉREQUIS

Bonnes connaissances de TCP/IP. Connaissances de base en sécurité informatique.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

1 Fonctionnement et installation

- Déploiements (distribué, standalone).
- Serveur de management (Security Management Server).
- Sauvegarde, restauration, snapshots et interface CLI.

Travaux pratiques

Installer Check Point sous Gaïa en version R81.

2 Politique de sécurité unifiée

- Règles, sous-règles par zone.
- Règles implicites, objets avec Object Explorer, l'anti-spoofing.

Travaux pratiques

Installer SmartConsole. Créer des objets et une politique de sécurité, des politiques partagées (shared policies). Gérer les tags.

3 Translation d'adresses (NAT)

- Règles et RFC 1918.
- NAT static/hide, ARP, VPN.
- Mode manuel, automatique.

Travaux pratiques

Mise en place de NAT automatique (type hide, static) et de règles de transaction manuelle.

4 VPN site à site et client vers site

- Principes du Réseau Privé Virtuel, IPSEC, IKEv1/v2, Software Blade Mobile Access.
- Mode traditionnel et simplifié.
- Client lourd Endpoint Security, Check Point Mobile.
- Authentification en Mobile Access : Check Point Mobile, Clients iOS/Android, Portail captif SSL Network Extender (SNX).

Travaux pratiques

Installer un tunnel IPsec site à site, un accès distant en VPN IPsec. Activation et mise en place de Check Point Mobile.

5 Firewall et gestion des utilisateurs

- Gérer des logs sur le Smartcenter, des alertes.
- Onglets Logs & Monitor, Gateways & Servers.
- Fonctionnalités SAM (Suspicious Activity Monitor) avec Check Point SmartView Monitor R81.
- Authentification des utilisateurs.
- Gestion de l'Identity Collector.
- Utilisation des Access Roles.

Travaux pratiques

Mise en oeuvre d'Identity Awareness, de l'examen et du filtrage des logs. Bloquer les intrusions avec SAM.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

- Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

6 Module IPS

- Vulnérabilités, failles de sécurité, référencement CVE.
- Profil de sécurité, politique IPS.

Exemple

Protection contre les vulnérabilités avec le module IPS.

7 Contrôle applicatif

- Notions de signatures applicatives.
- Créations d'applications personnalisées.
- Gestion des limites, des UserCheck, filtrage URL.

Exemple

Déploiement d'une politique de sécurité de contenu.

8 Threat Prevention

- Modules Antivirus, Antibot.
- Threat Extraction/Emulation.

Travaux pratiques

Mise en oeuvre d'une politique de Threat Prevention.

Dates et lieux

CLASSE À DISTANCE

2026 : 16 juin, 27 oct.