Formation **Check Point Certified Security Administrator R81.X**

Réussir l'examen de certification CCSA

A l'issue de cette formation CCSA de 3 jours, les participants ont acquis les connaissances et compétences nécessaires pour configurer et gérer les opérations quotidiennes de Check Point Security Gateway and Management Software Blades sur le système d'exploitation GAiA. Le coût de la certification est inclus dans le prix de la formation.

Durée

3 jours

Objectifs pédagogiques

- Installer Check Point R81 dans un environnement distribué
- Configurer les objets, règles et paramètres d'une politique de sécurité
- Travailler avec plusieurs administrateurs simultanés et définir des profils de permission
- Configurer un Réseau Privé Virtuel (VPN) et travailler avec le clustering Check Point
- Effectuer des tâches courantes d'administration
- Se préparer efficacement au passage de l'examen de certification CCSA

Public

Ingénieurs, techniciens et administrateurs systèmes et réseaux, RSSI.

Prérequis

Bonnes connaissances sur Windows, les systèmes UNIX, les technologies réseaux ainsi que sur Internet et le protocole TCP/IP. Une expérience d'au moins 6 mois avec les produits Check Point est vivement conseillée avant de passer l'examen.

Programme de formation

Introduction à la formation CCSA

Présentation générale de la formation certifiante Check Point Certified Security Administrator (CCSA)
Vue d'ensemble des technologies Check Point
L'intérêt d'obtenir une certification CCSA

Thèmes abordés

Les tâches courantes des administrateurs Check Point
Les fonctions de base du système d'exploitation Gaia
Les fonctionnalités, fonctions et ouils de la SmartConsole
Utilisation de la SmartConsole par les administrateurs pour gérer les droits d'accès

Principes de fonctionnement des produits et solutions de sécurité Check Point pour la protection des réseaux informatiques
Les licences et exigences contractuelles
Les éléments essentiels d'une politique de sécurité
Le concept Check Point de "policy layer"
Comment activer Application Control et URL Filtering
Utiliser les Blades pour bloquer l'accès à des applications
Configuration manuelle et automatique du NAT (Translation d'adresse réseau)
Identification des outils utilisés pour surveiller les données, déterminer les menaces et reconnaître les opportunités d'amélioration des performances
Les différentes solutions Check Point Threat Prevention pour les attaques réseau
Configuration, maintenance et tuning de l'Intrusion Prevention System
Le système Infinity Threat Prevention
Le système IoT Protect

Exercices pratiques réalisés pendant la formation

Configurer le Security Management Server
Utiliser l'interface Web pour exécuter le First Time Wizard
Installer la Smart Console
Installer la Alpha Gateway
Démontrer comment le Security Management Server et la Gateway communiquent
Tester le statut SIC
Créer plusieurs administrateurs et appliquer différents rôles et permissions pour l'administration simultanée
Valider les licences existantes pour les produits installés sur le réseau
Créer et configurer les objets hôte, réseau et groupe
Créer une politique de sécurité simplifiée
Utiliser les Security Zones
Partager une couche entre les politiques de sécurité
Configurer la translation d'adresses (NAT) pour les objets serveur et réseau
Activer l'Identity Awareness
Déployer les rôles d'accès utilisateur pour un contrôle plus granulaire de la politique de sécurité
Générer du trafic réseau et utiliser les outils de visibilité du trafic pour surveiller les données
Utiliser la Smart Console et SmartView Monitor pour visualiser les statuts, les alertes et bloquer le trafic suspect

Modalités d'évaluation

Nombre de questions : 100
Type de questions : QCM, basées sur des scénarios en situation réelle
Score requis : 70% de bonnes réponses