CCSA, Check Point Certified Security Administrator R81, préparation à la certification

Cours Pratique de 4 jours - 28h
Réf : CPQ - Prix 2024 : 3 280CHF HT

Cette formation vous permettra d'acquérir l'ensemble des techniques et des méthodologies nécessaires au passage de l'examen pour l'obtention de la certification CCSA R81. Vous apprendrez à mettre en place une politique de sécurité, la translation d'adresses (NAT) ou encore le module Intrusion Prevention System (IPS).

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Installer et configurer le produit Check Point R81

Mettre en œuvre la translation d'adresse (NAT)

Déployer une politique de sécurité et surveiller le trafic

Préparer l'examen officiel menant à la certification CCSA

Mettre en œuvre la politique de contrôle des applications, le filtrage d'URL et la gestion des utilisateurs

CERTIFICATION

Pour passer l'examen de certification, il suffit de vous inscrire sur le site de Check Point. Vous pouvez ensuite passer l'examen directement en ligne ou dans un centre agréé.

PARTICIPANTS

Techniciens, administrateurs et ingénieurs système/réseaux/sécurité.

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.

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 stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage 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 stagiaire 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

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 10/2022

1) Présentation de l'architecture Check Point R81

- Les produits Check Point.
- Nouveautés de la version R81.

2) Déploiement Gaia : Installation des « appliances » Check Point

- Présentation du système Gaïa.
- Eléments de l'architecture trois-tiers.
- Architecture modulaire des "Software Blades".
- Check Point Infinity.
- L'architecture en mode distribué et en mode standalone.
- Le serveur de management. Le protocole SIC.

Travaux pratiques : Installation de Check Point R81.

3) Gestion du Security Management Server

- Prise en main de SmartConsole R81.
- Politique de sécurité. Gestion des règles.
- Politiques Unifiées.
- Inspection des paquets.
- « Inline » Policies (sous règles).

Travaux pratiques : Installation de SmartConsole. Créer des objets. Réaliser une politique de sécurité. Activer l'anti-spoofing.

4) La translation d'adresses (NAT)

- Les règles de translation d'adresses avec IPv4 et IPv6.
- Le NAT statique (One To One NAT) et le NAT dynamique (Many To One NAT)/PAT.
- Le NAT Manuel.
- La problématique ARP et le routage.

Travaux pratiques : Mise en place de NAT automatique de type statique, Hide et règles de transaction manuelle.

5) Visibilité : gestion des logs, monitoring et reporting

- La politique de gestion des logs.
- Suivre les connexions avec Logs & Monitor (ancien SmartView Tracker).
- Le SmartView Monitor, fonctionnalités et seuils d'alerte.

Travaux pratiques : Activation du monitoring, utilisation du Suspicious Activity Monitoring Protocol, visualisation du trafic, monitoring de l'état de la politique de sécurité.

6) Gestion des licences et du Multi-Sites

- Structure de licences.
- Gestion de licences dans SmartUpdate et SmartConsole.
- Types de licences.
- Gestion de contrats et services.
- Monitoring le statut de licences.
- Définition de Policy Packages.
- Gestion de Policy Packages.
- Definition et types de “Layers”.
- Inspection des packets dans une « Ordered Layer ».
- Partage de « Layers » (Policy Layers Sharing).

7) Gestion d’administrateurs

- "Permission Profiles".
- Limiter la portée d'action des administrateurs.
- Gestion des utilisateurs concurrents.
- Gestion des sessions.

Travaux pratiques : Création d’un nouveau « Permission Profile » avec des autorisations limitées.

8) Déchiffrement HTTPS

- Création des règles.
- Gestion de certificats.
- Server Name Indications (SNI).

Travaux pratiques : Mise en œuvre de l’inspection HTTPS.

9) Contrôle Applicatif / Filtrage URL

- Les limites d'un firewall classique par IP et par port.
- Le contrôle d'accès.
- Le "AppWiki". L'URL Filtering.
- Le “User Check”.

Travaux pratiques : Filtrage Web et Applications : créer et partager la politique de « Filtrage Web et Applications » en tant que « Inline Layer » et « Ordered Layer ».

10) Politique à base d’utilisateurs/de « Threat Prevention »

- Besoin de récupérer l’identité des utilisateurs.
- Les méthodes d'authentification Identity Awareness R81.
- Les objets de type « Access Role ».
- La politique de Threat Prevention et ses « Software Blades ».
- Gestion des règles.
- Profils de sécurité.

- Autonomous Threat Prevention.
Travaux pratiques : Authentification : mise en place d'Identity Awareness, création de rôles et des accès.
Anti-Virus et Anti-Bot.

LES DATES

CLASSE À DISTANCE
2024 : 02 juil., 24 sept., 19 nov.