Date de publication : 28/05/2025

Formation : CCSE Check Point Certified Security Expert R82, certification

Formation pratique - 4j - 28h00 - Réf. CPK
Prix : 2890 CHF H.T.

NEW

La formation enseigne l'usage des APIs, la gestion des politiques de sécurité, VPN et performances réseau. Elle couvre le déchiffrement HTTPS, SmartEvent, l'authentification, et la haute disponibilité avec ElasticXL La formation prépare à la certification CCSE.

Objectifs pédagogiques

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

- Automatiser la gestion via API
- Effectuer des mises à niveau avancées
- Comprendre les processus internes Check Point et l'installation de la politique de sécurité
- Optimiser les performances réseau
- Configurer des VPN Domain-Based avec routage
- Mettre en œuvre l'accès distant sécurisé
- Superviser les événements et logs
- Déchiffrer le trafic HTTPS. Comprendre la gestion du protocole HTTP/3
- Gérer l'authentification d'utilisateurs
- Maîtriser la haute disponibilité et l'équilibrage de charge

Public concerné

Technicien, administrateur et ingénieur système/réseaux/sécurité.

Prérequis

Bonnes connaissances de TCP/IP, de la sécurité des SI et des principales fonctions de Check Point ou avoir suivi le cours "CCSA, Check Point Certified Security Administrator R82" (Réf. CPH).

PARTICIPANTS

Technicien, administrateur et ingénieur système/réseaux/sécurité.

PRÉREQUIS

Bonnes connaissances de TCP/IP, de la sécurité des SI et des principales fonctions de Check Point ou avoir suivi le cours "CCSA, Check Point Certified Security Administrator R82" (Réf. CPH).

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.

Méthodes et moyens pédagogiques

Exercice

Pédagogie active et participative à travers des exercices pratiques.

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

1 Administration avancée de Gaia & API

- Utilisation de l'interface CLI Gaia.
- Création d'objets et de règles via l'API.
- Automatisation avec les appels API REST.

Exercice

Installation du SMS et des GWs en R81.20. Utilisation de l'API pour créer des objets et règles de base.

2 Mise à niveau des systèmes Check Point

- Méthodes de mise à jour de Gaia.
- Upgrade centralisé des passerelles et serveurs de management.

Exercice

Mise à niveau avancée du Management de R81.20 vers R82. Mise à niveau centralisée de la passerelle principale et distante.

3 Les processus Check Point et installation de la politique de sécurité

- Fonctionnement des processus Check Point. Les commandes pour les visualiser
- Utilisation de SmartTasks avec des scripts pour l'automatisation.
- Installation accélérée de la politique de sécurité.
- Policy Packages, Layers, objets dynamiques, « Updatable Objects ».
- Introduction de « Dynamic Layer ». Communication directe avec la passerelle via l'API.

Exercice

Configure SmartTasks. Vérification des fichiers d'installation. Création des objets dynamiques. Utilisation du « Dynamic Layer » pour créer des objets et règles directement dans le firewall principal.

4 Optimisation des performances – SecureXL & CoreXL

- Accélération matérielle et logicielle.
- CoreXL Affinity, Dynamic Dispatcher, Hyperflow.

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.

5 VPN avancé – Routage Domain-Based

- VPN Domain-Based vs Route-Based.
- Surveillance des tunnels avec Network Probe.
- Wire Mode et méthodes d'authentification.

Exercice
.Mise en place du Routage VPN (Domain-Based).

6 Accès distant sécurisé

- VPN SSL/IPSec avec Mobile Access Blade.
- Authentification SAML et intégration Active Directory.

Exercice
Mise en place des connexions VPN de type « Remote Access » et SSL

7 Logs, monitoring et SmartEvent

- SmartEvent, SAM, ConnView.
- Reporting avancé et conformité.

Exercice
Configuration de SmartEvent.

8 Inspection HTTPS et sécurité applicative

- Déchiffrement HTTPS, SNI, HTTP/3 (QUIC).
- Modes de performance et gestion des certificats.

Exercice
Mise en oeuvre de l'inspection HTTPS.

9 Politique à base d'utilisateurs

- Identity Awareness, Access Roles.

Exercice
Authentification : mise en place d'Identity Awareness, création de rôles et des accès.

10 Clustering

- Haute disponibilité et « load sharing » avec ClusterXL et ElasticXL.

Exercice
Mise en œuvre de « Load Sharing » via ElasticXL.

Options

Certification : 300 € HT

La certification est délivrée par Check Point Software Technologies. Elle valide les compétences avancées nécessaires pour administrer, optimiser et sécuriser les infrastructures Check Point. La durée est de 90 minutes et repose sur un QCM de 90 questions, en anglais.

L'option de certification se présente sous la forme d'un voucher ou d'une convocation qui vous permettra de passer l'examen à l'issue de la formation.

Dates et lieux

CLASSE À DISTANCE
2026 : 23 juin, 6 oct., 15 déc.