Expert de la sécurité Check Point (CCSE) - V.R81.20

Date et durée

Code formation : CCSEFR
Durée : 3 jours
Nombre d'heures : 21 heures

Formation avec certification

CCSE : Certified Security Expert

Description

La cybersécurité est le socle indispensable des infrastructures numériques d'aujourd'hui, exigeant une expertise avancée pour architecturer et défendre les réseaux contre les menaces les plus sophistiquées. Une **maîtrise approfondie des solutions Check Point**, au-delà de l'administration de base, est cruciale pour concevoir des systèmes robustes, optimiser les performances de sécurité et garantir la résilience de votre organisation face aux cyberattaques complexes.
Notre **formation expert de la sécurité Check Point (CCSE)**, basée sur la version R81.20, vous offre une immersion complète dans les fonctions vitales d'ingénierie et d'optimisation des environnements de sécurité. Vous maîtriserez les déploiements avancés, la gestion de la haute disponibilité, l'optimisation des performances et la prévention personnalisée des menaces. Cela vous positionnera comme un expert recherché **en architecture et en dépannage Check Point**.
À l'issue de ce programme de 3 jours, vous maîtriserez les compétences clés pour **réussir l'examen de certification Certified Security Expert (CCSE)** (*en savoir plus dans l'onglet certification*). Vous bénéficierez d'une préparation approfondie, incluant des travaux pratiques complexes et des conseils d'experts, pour vous assurer une réussite optimale et une reconnaissance officielle de votre expertise en tant qu'**ingénieur de sécurité Check Point**.

Objectifs

À l'issue de cette formation Check Point CCSE, vous atteindrez les objectifs suivants :

- maîtriser les interfaces principales utilisées pour la gestion avancée de l'environnement Check Point ;
- identifier et exploiter les technologies Check Point supportant l'automatisation de la sécurité ;
- expliquer le but et la mise en œuvre du déploiement Check Management en Haute Disponibilité (HA) ;
- déployer une solution de serveurs primaire et secondaire en suivant le flux de travail recommandé ;
- expliquer et configurer les concepts fondamentaux du Clustering et de ClusterXL, y compris les protocoles, la synchronisation et la persistance des connexions ;
- identifier comment exclure des services de la synchronisation ou gérer son délai ;
- expliquer le flux d'installation des politiques de sécurité ;
- maîtriser l'utilisation des objets dynamiques, des objets actualisables et des flux réseau dans les politiques de sécurité ;
- comprendre comment gérer l'accès des utilisateurs, qu'ils soient internes ou externes ;
- décrire et déployer les composants et configurations d'Identity Awareness ;
- décrire les différentes solutions de prévention des menaces offertes par Check Point ;
- articuler et configurer le système de prévention des intrusions (IPS) ;

- acquérir des connaissances sur la protection IoT (Internet des Objets) de Check Point ;
- expliquer l'objectif et les configurations des VPN basés sur des domaines ;
- décrire les scénarios où l'authentification par certificat gérée en externe est appropriée ;
- fournir la sécurité client via l'accès à distance et comprendre ses mécanismes ;
- maîtriser l'utilisation du logiciel Mobile Access Software Blade ;
- déterminer la conformité de la configuration avec les meilleures pratiques de sécurité Check Point ;
- définir les solutions d'optimisation des performances et le flux de travail de configuration de base ;
- identifier et appliquer les méthodes et procédures de mise à niveau et de migration prises en charge pour les serveurs Security Management, les serveurs dédiés de journaux et SmartEvent ;
- identifier et appliquer les méthodes et procédures de mise à niveau prises en charge pour les Security Gateways ;
- se préparer efficacement à l'examen de certification Certified Security Expert (CCSE) pour valider votre expertise.

Points forts

- **Formateurs experts et certifiés Check Point :** bénéficiez de l'expérience de formateurs certifiés par Check Point et fortement expérimentés dans la conception, le déploiement, la maintenance et le support d'architectures de sécurité Check Point complexes en environnement réel.
- **Contenu officiel Check Point et support complet :** accédez aux supports pédagogiques officiels de Check Point pour la version R81.20, garantissant une compréhension approfondie et à jour de la plateforme au niveau expert.
- **Pédagogie orientée pratique et avancée :** renforcez vos compétences techniques grâce à de nombreux travaux pratiques, incluant des scénarios complexes de déploiement et de dépannage, conçus pour l'application directe des concepts d'ingénierie et d'optimisation Check Point.
- **Préparation intensive à la certification CCSE :** maximisez vos chances de succès à l'examen avec des révisions ciblées et des conseils d'experts, vous préparant spécifiquement à la certification Certified Security Expert (CCSE).

Certification

Cette formation vous prépare de manière intensive à l'examen de certification Certified Security Expert (CCSE) de Check Point. Un code coupon vous sera fourni à la fin du cours pour que vous puissiez programmer votre examen.

Modalités de l'examen CCSE :

- **Type d'examen :** QCM
- **Nombre de questions :** 90
- **Lieu :** centres de test accrédités Pearson VUE ou via une surveillance en ligne
- **Langue :** anglais
- **Durée :** 90 minutes (*15 minutes supplémentaires peuvent être accordées pour les candidats dont l'anglais n'est pas la langue maternelle*).
- **Note de passage :** 70%

Notre formation vous fournira les connaissances approfondies et les compétences pratiques nécessaires pour aborder l'examen avec confiance. En réussissant cet examen, vous obtiendrez la certification Certified Security Expert (CCSE), une reconnaissance officielle de votre expertise avancée en sécurité Check Point.
À savoir : *l*a certification CCSE a une durée de validité de **2 ans**. Pour maintenir votre statut de certifié CCSE, vous avez la possibilité de :

- **Repasser l'examen CCSE** actuel (référence 156-315.81.20) avant la date d'expiration de votre certification.

- **Obtenir la certification de niveau supérieur (CCSM ou CCSM Elite)** pendant que votre certification CCSE est encore valide, ce qui maintiendra de fait votre statut de certifié Check Point.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- avoir suivi la formation Administrateur de la sécurité Check Point (CCSA) ou posséder la certification Check Point Certified Security Administrator en cours de validité ;
- **posséder une connaissance pratique des systèmes d'exploitation courants**, qu'il s'agisse de Windows ou de systèmes de type Unix (comme Linux) ;
- **avoir une expérience pratique de la gestion des certificats numériques**, incluant les concepts clés (clés publiques/privées et autorités de certification) ;
- **posséder une connaissance solide en administration système et réseau**, couvrant des aspects tels que la gestion sur Windows et Unix/Linux, le routage avancé et la segmentation réseau ;
- **savoir lire et comprendre l'anglais technique** pour accéder au support de cours officiel et au passage de l'examen CCSE.

Public

Cette formation s'adresse aux publics suivants :

- **les professionnels techniques de la cybersécurité** qui sont directement impliqués dans la conception, le déploiement, la mise à niveau, la maintenance ou le support des architectures et des infrastructures de sécurité Check Point complexes. Les rôles typiques peuvent inclure (sans s'y limiter) :
    - Ingénieur Sécurité confirmé
    - Architecte Sécurité
    - Expert Cybersécurité
    - Consultant en Sécurité (spécialisé en intégration et optimisation)
    - Administrateur Sécurité senior ;
- **les professionnels de l'IT et des réseaux** qui cherchent à approfondir leur expertise en cybersécurité, à se spécialiser sur les technologies Check Point à un niveau avancé, ou à valider des compétences pointues en ingénierie et dépannage de solutions de sécurité ;
- **les responsables d'équipes techniques ou chefs de projet** qui supervisent des projets d'architecture, de déploiement d'envergure ou d'optimisation des infrastructures de sécurité Check Point, et qui nécessitent une compréhension technique experte pour la prise de décision stratégique ;
- **toute personne qui souhaite obtenir la certification Certified Security Expert (CCSE)** pour valider ses compétences avancées, renforcer sa crédibilité et accélérer sa progression professionnelle vers des rôles d'expert en cybersécurité.

Programme

Module 1 : gérer les déploiements avancés

- Le déploiement avancé des environnements de sécurité Check Point.
- La gestion de la haute disponibilité du management (Management High Availability).
- Le déploiement avancé des passerelles (gateways).

Travaux pratiques :

- Déployer un serveur secondaire de gestion de la sécurité.
- Configurer un serveur de logs dédié.
- Déployer SmartEven.

Module 2 : configurer les politiques avancées et la gestion des accès

- La configuration avancée des politiques de sécurité.
- La gestion avancée de l'accès utilisateur.
- La protection personnalisée contre les menaces.

Travaux pratiques :

- Configurer un cluster de passerelle de sécurité à haute disponibilité.
- Travailler avec ClusterXL.
- Configurer des objets dynamiques et actualisables.
- Vérifier l'installation accélérée de la politique et le statut de surveillance.
- Déployer Identity Awareness.
- Personnaliser la prévention des menaces.

Module 3 : maîtriser les VPN et l'accès mobile

- Le déploiement de VPN Site-to-Site avancés.
- Le déploiement de VPN Remote Access.
- La gestion de Mobile Access VPN.

Travaux pratiques :

- Configurer un Site-to-Site VPN avec un Interoperable Device.
- Déployer Remote Access VPN.
- Configurer Mobile Access VPN.

Module 4 : optimiser la surveillance et la performance

- La surveillance avancée de la sécurité.
- Le réglage des performances avancées.

Travaux pratiques :

- Surveiller la conformité des politiques (Monitoring Policy Compliance).
- Rapporter des statistiques SmartEvent (Reporting SmartEvent Statistics).
- Optimiser les performances du Security Gateway (Tuning Security Gateway Performance).
- Élever la sécurité avec l'inspection HTTPS (Elevating Security with HTTPS Inspection).

Module 5 : assurer la maintenance et les mises à niveau

- La maintenance avancée de la sécurité.
- L'identification des méthodes de mise à niveau et de migration supportées pour les serveurs Security Management, les serveurs de logs dédiés et les serveurs SmartEvent.
- L'identification des méthodes et procédures de mise à niveau supportées pour les Security Gateways.

Module 6 : se préparer à l'examen Certified Security Expert (CCSE)

- Révision approfondie des concepts clés abordés dans tous les modules.
- Ressources supplémentaires pour l'examen Certified Security Expert (CCSE).
- Stratégies et conseils pour maximiser ses chances de réussite à l'examen.