Administrateur de la sécurité Check Point (CCSA) - V.R81.20

Date et durée

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

Formation avec certification

CCSA : Certified Security Administrator

Description

La sécurité des systèmes d'information est devenue la pierre angulaire de toute infrastructure numérique moderne, protégeant les données et les réseaux contre un paysage de menaces en constante évolution. Une **maîtrise approfondie de l'administration de la sécurité**, et plus spécifiquement des solutions de pointe, comme celles de Check Point, est essentielle pour garantir la continuité des opérations, défendre les actifs numériques et maintenir la confiance de votre organisation face aux cyberattaques.
Notre **formation administrateur de la sécurité Check Point (CCSA)**, basée sur la version R81.20, vous offre une immersion complète dans les fonctions vitales de gestion des firewalls. Vous maîtriserez la configuration des politiques de sécurité, le contrôle d'applications, la gestion des VPN et la prévention des menaces avancées. Cela vous positionnera comme un spécialiste recherché en **cybersécurité Check Point**.
À l'issue de ce programme de 3 jours, vous maîtriserez les compétences clés pour **réussir l'examen de certification Certified Security Administrator** (*en savoir plus dans l'onglet certification)*. Vous bénéficierez d'une préparation approfondie, incluant de nombreux travaux pratiques et des conseils ciblés, pour vous assurer une réussite optimale et une reconnaissance officielle de votre expertise en tant qu'**administrateur de sécurité Check Point**.
Pour en savoir plus sur les modalités de certification, consultez notre section Certification.

Objectifs

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

- maîtriser les composants essentiels d'une architecture Check Point à 3 niveaux et comprendre leur interaction pour une gestion sécurisée de l'environnement ;
- expliquer et sécuriser la communication, tout en gérant efficacement le routage du trafic au sein de l'environnement Check Point ;
- décrire les fonctions fondamentales du système d'exploitation Gaia et ses capacités d'administration ;
- déployer SmartConsole et installer un Security Management Server ainsi qu'un Security Gateway pour mettre en place une solution de sécurité à domaine unique ;
- créer des objets SmartConsole pertinents pour modéliser la topologie de votre organisation et les intégrer dans les politiques et règles de sécurité ;
- identifier et utiliser les outils de gestion des licences et des contrats Check Point, en comprenant leur rôle et leur application pratique ;
- configurer et optimiser la politique de sécurité en exploitant les fonctionnalités et capacités avancées offertes ;

- comprendre l'impact des couches de politique sur l'inspection du trafic et savoir comment les agencer pour une sécurité optimale ;
- articuler l'effet de la traduction d'adresses réseau (NAT) sur le trafic et être capable de configurer la NAT manuelle et automatique ;
- maitriser le fonctionnement du contrôle d'applications, du filtrage d'URL et des capacités de prévention autonome des menaces, en configurant ces solutions selon les exigences de sécurité de votre organisation ;
- configurer les clés pré-partagées et les certificats pour authentifier les passerelles VPN tierces et externes, assurant ainsi une connectivité sécurisée ;
- analyser et interpréter le trafic des tunnels VPN pour diagnostiquer et résoudre les problèmes de connectivité sécurisée ;
- gérer les paramètres de journalisation et utiliser des requêtes personnalisées pour filtrer et analyser les résultats des journaux efficacement ;
- surveiller la santé du matériel Check Point via le portail Gaia et la ligne de commande pour anticiper et résoudre les problèmes ;
- mettre en œuvre les différentes méthodes de sauvegarde des informations du système Check Point, en appliquant les meilleures pratiques et recommandations pour la résilience de votre environnement ;
- se préparer efficacement à l'examen de certification Certified Security Administrator (CCSA) 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 mise en œuvre concrète et l'administration de solutions de sécurité en environnement réel.
- **Contenu officiel Check Point et support complet (Version R81.20) :** accédez aux supports pédagogiques officiels de Check Point pour la version R81.20, garantissant une compréhension approfondie et à jour de la plateforme.
- **Pédagogie orientée pratique :** renforcez vos compétences techniques grâce à de nombreux travaux pratiques) conçus pour l'application directe des concepts d'administration et de configuration de Check Point.
- **Préparation intensive à la certification CCSA :** maximisez vos chances de succès à l'examen avec des révisions ciblées et des conseils, vous préparant spécifiquement à la certification Certified Security Administrator (CCSA).

Certification

*Cette formation vous prépare de manière intensive à l'examen de certification Certified Security Administrator (CCSA**)** 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 CCSA :

- **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 Administrator (CCSA), une reconnaissance officielle de votre expertise en administration de la sécurité Check Point.

À savoir : *la certification CCSA a une durée de validité de* ***2 ans.*** Pour maintenir votre statut de certifié CCSA, vous avez la possibilité de :

- **Repasser l'examen CCSA** actuel (référence 156-215.81.20) avant la date d'expiration de votre certification.
- **Obtenir la certification de niveau supérieur (CCSE)** pendant que votre certification CCSA 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 :

- **posséder une connaissance pratique des systèmes d'exploitation courants**, qu'il s'agisse de Windows ou de systèmes de type Unix (comme Linux) ;
- **comprendre les concepts fondamentaux des réseaux TCP/IP,** incluant l'adressage IP, le routage et les principaux protocoles réseau ;
- **savoir lire et comprendre l'anglais technique** pour accéder au support de cours officiel et au passage de l'examen CCSA.

Public

Cette formation s'adresse aux publics suivants :

- **les professionnels techniques de la cybersécurité** qui sont directement impliqués dans la mise en œuvre, la maintenance, le support ou l'administration quotidienne des solutions de sécurité Check Point. Les rôles typiques peuvent inclure (sans s'y limiter) :
    - Administrateur sécurité
    - Ingénieur sécurité
    - Technicien réseau et sécurité
    - Analyste SOC (Centre d'Opérations de Sécurité)
    - Consultant en cybersécurité (impliqué dans le déploiement).
- **les professionnels de l'IT et des réseaux** qui cherchent à étendre leurs compétences vers la cybersécurité, à se spécialiser sur les technologies Check Point, ou à valider une expertise reconnue dans l'administration des firewalls et des politiques de sécurité ;
- **les responsables d'équipes techniques ou chefs de projet** qui supervisent des projets de déploiement ou de gestion des infrastructures de sécurité Check Point et qui nécessitent une compréhension opérationnelle approfondie des systèmes et de leurs capacités ;
- **toute personne qui souhaite obtenir la certification Certified Security Administrator (CCSA)** pour valider ses compétences, renforcer sa crédibilité et accélérer sa progression professionnelle dans le domaine de la cybersécurité.

Programme

Module 1 : démarrer avec l'environnement Check Point

- Présentation de l'architecture Check Point à 3 niveaux et interaction des composants.
- La sécurisation de la communication et du routage du trafic dans l'environnement Check Point.
- Les fonctions de base du système d'exploitation Gaia.
- Le déploiement de SmartConsole.

- L'installation de Security Management Server.
- L'installation du Security Gateway pour une solution à domaine unique.

Travaux pratiques :

- Déployer SmartConsole.
- Installer Security Management Server.
- Installer Security Gateway.

Module 2 : gérer les objets et les licences

- La création d'objets SmartConsole correspondants à la topologie de l'organisation.
- La gestion des licences et des contrats Check Point (outils, objectif et utilisation).

Travaux pratiques :

- Configurer des objets dans SmartConsole.
- Gérer les licences.
- Établir une communication interne sécurisée.

Module 3 : configurer les politiques de sécurité et la NAT

- Les fonctionnalités et les capacités avancées pour la configuration et la gestion de la politique de sécurité.
- L'impact des couches de politique sur l'inspection du trafic.
- La Traduction d'Adresses Réseau (NAT) (impact sur le trafic, configuration manuelle et automatique).

Travaux pratiques :

- Créer une politique de sécurité.
- Configurer les couches d'ordre.
- Configurer la NAT.
- Configurer une couche inline partagée.
- Intégrer la sécurité avec une politique unifiée.

Module 4 : contrôler les applications, filtrer les URL et prévenir les menaces

- La configuration d'Application Control & URL Filtering et des capacités de prévention autonome des menaces.

Travaux pratiques :

- Élever la sécurité avec la prévention autonome des menaces.

Module 5 : gérer les VPN et la Journalisation

- La configuration des clés pré-partagées et la gestion des certificats pour l'authentification avec les passerelles VPN tierces et externes.
- L'analyse et l'interprétation du trafic des tunnels VPN.
- La configuration des paramètres de journalisation.
- L'utilisation de requêtes prédéfinies et personnalisées pour filtrer les résultats des journaux.

Travaux pratiques :

- Configurer un VPN Site-to-Site géré localement.
- Élever la vue du trafic.

Module 6 : surveiller et maintenir l'environnement

- La surveillance de la santé du matériel Check Point via le Portail Gaia et la ligne de commande.
- Les méthodes de sauvegarde des informations système Check Point (différentes approches, meilleures pratiques et recommandations).

Travaux pratiques :

- Surveiller les états du système.
- Maintenir l'environnement de sécurité.
- Gérer l'accès administrateur.

Module 7 : se préparer à l'examen Check Point CCSA

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

Certified Security Administrator (CCSA) et Check Point sont des marques déposées de Check Point Software Technologies Ltd. ou de ses filiales aux États-Unis et/ou dans d'autres pays.
Pearson VUE est une marque déposée de Pearson Education, Inc. ou de ses sociétés affiliées.
Windows est une marque déposée du groupe de sociétés Microsoft.
Unix est une marque déposée de The Open Group.
Toutes les autres marques commerciales mentionnées sont la propriété de leurs détenteurs respectifs.