+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 02/10/2025

S'inscrire

Formation CCSE certification

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

4 jours (28 heures)

Présentation

La certification CCSE (Check Point Certified Security Expert) est une référence avancée en cybersécurité. Elle valide les compétences nécessaires pour déployer, administrer et dépanner des environnements complexes basés sur les solutions Check Point R81.20.

Notre formation CCSE vous permettra de maîtriser la sécurité avancée, les VPN multi-sites, la haute disponibilité, le clustering et la gestion multi-domaines. Les participants pourront exploiter les outils de diagnostic avancé, automatiser la détection des menaces et mettre en place des stratégies de continuité de service robustes.

Grâce à une approche pratique et progressive, vous serez en mesure de sécuriser des infrastructures critiques, de diagnostiquer efficacement des incidents complexes et de préparer avec confiance l'examen CCSE R81.20.

Cette certification internationale constitue un véritable tremplin de carrière pour les professionnels de la sécurité avancée.

Comme toutes nos formations, celle-ci s'appuie sur la dernière version stable de l'écosystème Check Point et privilégie une mise en situation concrète.

Objectifs

- Déployer et administrer des environnements Check Point avancés.
- Maîtriser la configuration des VPN multi-sites et du Remote Access.
- Assurer la haute disponibilité avec ClusterXL et Load Sharing.
- Exploiter les modules de Threat Prevention et l'inspection HTTPS.
- Diagnostiquer et résoudre des incidents complexes.
- Réussir la certification CCSE R81.20.

Public visé

- Ingénieurs en cybersécurité
- Administrateurs réseau expérimentés
- Analystes SOC de niveau avancé
- Consultants en sécurité IT

Pré-requis

- Certification CCSA R81.x ou expérience équivalente sur Check Point
- Bonne maîtrise des réseaux TCP/IP et des concepts de pare-feu
- Notions en VPN et en authentification

Programme de formation CCSE

[Jour 1 - Matin]

Introduction au CCSE et rappels avancés

- Présentation de la certification CCSE et son positionnement
- Rappel des fondamentaux CCSA : objets, politiques, NAT, VPN
- Nouveautés et fonctionnalités avancées R81.20
- Préparation de l’environnement de lab avancé
- Atelier pratique : Mise en place de l’environnement CCSE.

[Jour 1 - Après-midi]

Gestion avancée des politiques de sécurité

- Politiques granulaires et règles avancées
- Politiques multiples et gestion distribuée
- Contrôle des applications et prévention des menaces
- Optimisation et audit des politiques
- Atelier pratique : Implémentation de règles complexes.

Authentification et Identity Awareness avancée

- Intégration AD/LDAP avancée
- Authentification multi-facteurs et fédérée
- Règles basées sur l’identité et sur les rôles
- Analyse et dépannage des accès utilisateurs
- Atelier pratique : Configuration d’un SSO avec Identity Awareness.

[Jour 2 - Matin]

NAT avancé et troubleshooting réseau

- Scénarios avancés de NAT et flux complexes
- Gestion des collisions et limitations NAT
- Dépannage avec fw monitor, tcpdump, cpview
- Optimisation des performances NAT
- Atelier pratique : Analyse et résolution d’un incident NAT.

[Jour 2 - Après-midi]

Gestion des journaux et événements

- Utilisation avancée de SmartEvent et corrélation
- Mise en place d’alertes dynamiques
- Rapports personnalisés et conformité réglementaire
- Intégration avec un SIEM externe
- Atelier pratique : Création d’un tableau de bord avancé.

VPN avancés et architectures sécurisées

- VPN site-to-site avancés : topologies complexes
- VPN Remote Access avec haute disponibilité
- Sécurisation des tunnels et troubleshooting
- Intégration multi-fournisseurs
- Atelier pratique : Déploiement d’un VPN multi-sites.

[Jour 3 - Matin]

Haute disponibilité et ClusterXL avancé

- Modes avancés de ClusterXL et Load Sharing
- Gestion des upgrades avec cluster actif
- Troubleshooting des synchronisations d’état
- Résilience et continuité de service
- Atelier pratique : Simulation d’incidents et validation failover.

[Jour 3 - Après-midi]

Threat Prevention et protections avancées

- Configuration avancée des modules IPS, Anti-Bot, AV
- Inspection HTTPS avancée
- Optimisation des signatures et performance
- Analyse et réponse automatisée aux menaces
- Atelier pratique : Réponse à un scénario d’attaque.

Administration centralisée et multi-domaines

- Concepts de Multi-Domain Security Management (MDM)
- Gestion avancée des administrateurs et permissions
- Migration et reprise après incident
- Sauvegarde et restauration avancées
- Atelier pratique : Scénarios multi-domaines complexes.

[Jour 4 - Matin]

Dépannage et diagnostic avancé

- Méthodologie de troubleshooting avancé
- Outils : cpinfo, fw monitor, kernel debug
- Cas pratiques : VPN, NAT, Cluster et politiques
- Mise en œuvre d’un runbook de troubleshooting
- Atelier pratique : Résolution d’incidents multi-protocoles.

[Jour 4 - Après-midi]

Mise en production et durabilité

- Checklist de durcissement pour la production
- Gestion des upgrades et Jumbos Hotfix
- Optimisation des performances système
- Bonnes pratiques de monitoring avancé
- Atelier pratique : Passage simulé en production.

Préparation à la certification CCSE

- Structure et format de l’examen CCSE R81.20
- Thèmes clés et pondération par section
- Stratégies de révision et tests blancs
- Conseils pratiques pour l’examen officiel
- Atelier pratique : Passage de l'examen blanc + correction.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes,

souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.