+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 CCSM certification

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

La certification CCSM (Check Point Certified Security Master) est le niveau le plus avancé du parcours Check Point. Elle atteste d'une expertise approfondie en cybersécurité, en conception d'architectures complexes et en résolution d'incidents critiques.

Notre formation CCSM vous permettra de développer une maîtrise complète des environnements Check Point R81.20. Vous apprendrez à gérer des architectures distribuées, des scénarios de VPN multi-sites, la haute disponibilité multi-datacenters, l'automatisation via API et la réponse à des attaques avancées.

Avec une approche résolument pratique, vous serez en mesure de concevoir, administrer et dépanner des infrastructures de sécurité critiques tout en vous préparant à la certification CCSM R81.20.

Cette certification internationale est reconnue comme un véritable gage de maîtrise et ouvre la voie aux rôles d'architecte sécurité et d'expert SOC.

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

Objectifs

- Concevoir et administrer des environnements Check Point complexes.
- Optimiser la haute disponibilité et les scénarios de clustering multi-sites.
- Déployer et sécuriser des VPN avancés et architectures hybrides.
- Automatiser la sécurité via API et intégrations DevSecOps.
- Mener des investigations forensic et du threat hunting avancé.
- Réussir la certification CCSM R81.20.

Public visé

- Ingénieurs sécurité senior
- Architectes en cybersécurité
- Responsables SOC
- Consultants experts en sécurité IT

Pré-requis

- Certification CCSE R81.x fortement conseillé (ou expérience équivalente)
- Solides compétences en réseaux TCP/IP et en cybersécurité
- Expérience confirmée dans l’administration de solutions Check Point

Programme de Formation CCSM

[Jour 1 - Matin]

Introduction au CCSM et rappels avancés

- Présentation de la certification CCSM et son positionnement
- Prérequis : maîtrise des concepts CCSA/CCSE
- Objectifs et attentes de l’examen CCSM R81.20
- Présentation de l’environnement de lab avancé
- Atelier pratique : Mise en place du lab de formation CCSM.

[Jour 1 - Après-midi]

Politiques avancées et optimisations

- Gestion des politiques complexes et règles avancées
- Segmentation de la sécurité et domaines multiples
- Analyse de performance des politiques
- Automatisation de la gestion des règles
- Atelier pratique : Optimisation d’une politique sur un environnement large.

Authentification et contrôle d’accès avancés

- Intégration avec SSO, SAML, MFA
- Contrôle d’accès basé sur l’identité et le contexte
- Troubleshooting des environnements hybrides
- Gestion avancée des logs d’authentification
- Atelier pratique : Intégration MFA avec un SI externe.

[Jour 2 - Matin]

Traduction d’adresses et routage avancé

- NAT avancé : scénarios complexes et exceptions
- Routage dynamique et intégration avec BGP/OSPF
- Analyse des flux hybrides (cloud + on-prem)
- Dépannage avancé de la translation et du routage
- Atelier pratique : Mise en œuvre d’un routage dynamique avec NAT complexe.

[Jour 2 - Après-midi]

Monitoring et observabilité avancée

- Logs et corrélations avancées
- SmartEvent et dashboards personnalisés
- Intégration avec un SIEM d’entreprise
- Supervision proactive et capacity planning
- Atelier pratique : Création d’un SOC dashboard complet.

VPN avancés et architectures distribuées

- VPN site-to-site avancés (redondance, multi-hubs)
- Remote Access VPN : scalabilité et durcissement
- Troubleshooting complexe VPN IPSec
- Sécurité hybride cloud + on-prem avec VPN
- Atelier pratique : Mise en place d’un VPN distribué multi-sites.

[Jour 3 - Matin]

Haute disponibilité avancée

- ClusterXL : scénarios complexes et multi-datacenters
- Synchronisation multi-niveaux et dépannage cluster
- Maintenance et upgrades sans interruption
- Stratégies de résilience et reprise après sinistre
- Atelier pratique : Simulation d’incidents et failover distribué.

[Jour 3 - Après-midi]

Threat Prevention avancée

- Optimisation IPS/Anti-Bot/Threat Emulation
- Inspection HTTPS complète et contraintes
- Performance et tuning des signatures
- Scénarios d’attaque complexes et réponse
- Atelier pratique : Tuning et réponse à un scénario APT.

Automatisation et API

- Utilisation avancée de l’API Check Point
- Scripting et intégration DevSecOps
- Gestion automatisée des règles et objets
- Sécurité as Code et orchestration
- Atelier pratique : Automatisation d’un déploiement via API.

[Jour 4 - Matin]

Forensic et investigation

- Collecte de preuves et logs avancés
- Outils forensic Check Point
- Analyse d’incidents et Threat Hunting
- Rédaction d’un rapport post-incident
- Atelier pratique : Simulation d’une investigation SOC.

[Jour 4 - Après-midi]

Multi-domain et architectures complexes

- Concepts avancés de Multi-Domain Security Management (MDM)
- Scénarios hybrides et multi-clients
- Gestion des rôles et permissions
- Migration et continuité d’activité
- Atelier pratique : Déploiement multi-domaines complexe.

Troubleshooting avancé

- Méthodologie de troubleshooting expert
- Outils avancés : fw monitor, cpview, kernel debug
- Diagnostic cluster, VPN, NAT et policies
- Détection proactive d’anomalies
- Atelier pratique : Résolution d’incidents multi-couches.

[Jour 5 - Matin]

Sécurité cloud et hybride

- Intégration avec AWS, Azure et GCP
- Check Point CloudGuard et orchestration hybride
- Cas d’usage cloud natifs et hybrides
- Sécurité avancée des workloads cloud
- Atelier pratique : Sécurisation d’une infra hybride.

[Jour 5 - Après-midi]

Mise en production et durabilité

- Préparation et checklist de go-live
- Maintenance et upgrade avancés
- Tuning performance et scalabilité
- Bonnes pratiques FinOps et gouvernance
- Atelier pratique : Déploiement simulé et suivi.

Préparation à la certification CCSM

- Structure de l’examen officiel CCSM R81.20
- Thèmes clés et pondération par domaine
- Stratégie de préparation et révision finale
- Simulation d’examen et pièges à éviter
- 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.