+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 CCSA certification

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

4 jours (28 heures)

Présentation

La certification CCSA (Check Point Certified Security Administrator) est une référence de la cybersécurité. Elle valide la capacité à déployer, configurer et administrer une solution Check Point dans un environnement d'entreprise.

Notre formation CCSA vous permettra de maîtriser la gestion des politiques, la configuration des VPN, la traduction d'adresses (NAT), la surveillance et l'implémentation d'architectures haute disponibilité.

Vous mettrez en œuvre les outils de diagnostic et les modules avancés (IPS, Anti-Virus, Anti-Bot) pour une protection opérationnelle.

Par une approche résolument pratique, vous consoliderez les compétences nécessaires pour sécuriser des réseaux modernes tout en vous préparant au passage de la certification CCSA R81.x.

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

Objectifs

- Administrer une infrastructure Check Point de bout en bout.
- Concevoir et déployer des politiques de sécurité efficaces.
- Configurer et dépanner les VPN site-to-site et remote access.
- Assurer la haute disponibilité et la résilience.
- Exploiter les outils de monitoring et de troubleshooting.
- Réussir l'examen CCSA R81.x.

Public visé

- Administrateurs systèmes et réseaux
- Ingénieurs et analystes Sécurité / SOC
- Consultants et techniciens sécurité

Pré-requis

- Connaissances de base en TCP/IP et en sécurité
- Première expérience avec un pare-feu

Programme de formation CCSA

[Jour 1 - Matin]

Introduction à l’écosystème Check Point et à la certification

- Panorama des solutions Check Point et versions R81.x
- Rappels réseaux TCP/IP et principes de pare-feu stateful
- Architecture Security Gateway et Security Management
- Découverte de SmartConsole et des principaux blades
- Atelier pratique : Première connexion, inventaire et repérage des menus.

[Jour 1 - Après-midi]

Objets, politiques et déploiements

- Création d’objets réseau, services et utilisateurs
- Conception d’une politique de sécurité robuste
- Gestion des installations de politique et des sessions
- Bonnes pratiques de segmentation et durcissement
- Atelier pratique : Écrire, valider et déployer une politique initiale.

Contrôle d’accès et identité

- Intégration LDAP/RADIUS/TACACS+ et Identity Awareness
- Règles basées utilisateur/groupe et contrôles applicatifs
- Logs d’authentification, corrélation et audit
- Mises en garde : héritage, groupes dynamiques, priorités
- Atelier pratique : Accès conditionnel par groupe AD.

[Jour 2 - Matin]

Traduction d’adresses (NAT) et flux

- Modèles NAT : statique, dynamique, hide NAT
- Ordre d’évaluation des règles et résolution des collisions
- Lecture des logs et traçage de flux
- Pièges courants : asymétrie, ports éphémères, PAT
- Atelier pratique : Scénarios NAT et validation de connectivité.

[Jour 2 - Après-midi]

Journaux, visibilité et détection

- Exploitation de SmartLog et SmartEvent
- Recherches avancées, rapports, tableaux de bord
- Alerting et intégration SIEM
- Traçabilité et conformité : rétention et sauvegardes
- Atelier pratique : Analyse d’incident de bout en bout.

VPN site-to-site et accès distant

- Concepts IPsec (phases, crypto, PFS, lifetimes)
- Configuration d’un VPN site-to-site
- Remote Access VPN : profils, déploiement client
- Dépannage : négociation IKE, sélection d’intéressants, routage
- Atelier pratique : Mise en place d’un tunnel inter-sites.

[Jour 3 - Matin]

Haute disponibilité et ClusterXL

- Modes HA et Load Sharing, topologies et prérequis
- Configuration ClusterXL et synchronisation d’état
- Tests de failover et validation applicative
- Maintenance : paquets, upgrades, fenêtres de changement
- Atelier pratique : Cluster à deux nœuds et bascule contrôlée.

[Jour 3 - Après-midi]

Threat Prevention et sécurité avancée

- Modules IPS, Anti-Bot, Anti-Virus, App Control, URL Filtering
- Profils, exceptions, mises à jour et performance
- Inspection du trafic HTTPS (TLS) : impacts et bonnes pratiques
- Analyse et réponse aux menaces
- Atelier pratique : Durcir un environnement contre une attaque simulée.

Administration et gouvernance

- Rôles, permissions et délégation d’administration
- Sauvegarde/restore, snapshots, export de configuration
- Gestion des licences et du support
- Conformité & politiques globales
- Atelier pratique : Sauvegardes et reprise après incident.

[Jour 4 - Matin]

Dépannage et outils d’analyse

- Méthodologie de troubleshooting
- Outils : cpview, tcpdump, fw monitor
- Diagnostics VPN/NAT/HA : cas typiques
- Collecte d’archives de support et bonnes pratiques
- Atelier pratique : Résolution guidée d’incidents multi-domaines.

[Jour 4 - Après-midi]

Mise en production et exploitation

- Checklist go-live : sécurité, sauvegardes, supervision
- Stratégies d’upgrade et de maintenance
- Intégrations cloud/hybride et segmentation
- Mesure de performance et capacity planning
- Atelier pratique : Runbook d’exploitation et tableau de bord.

Préparation à la certification CCSA R81.x

- Format de l’examen, thèmes clés et pondération
- Stratégies de révision, pièges et gestion du temps
- Ressources officielles et labs
- Plan d’action personnalisé
- 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.