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

Updated on 02/10/2025

Sign up

CCSM certification training

ALL-IN-ONE : EXAM INCLUDED IN PRICE

5 days (35 hours)

Overview

CCSM (Check Point Certified Security Master) certification is the most advanced level in the Check Point curriculum. It certifies in-depth expertise in cybersecurity, complex architecture design and critical incident resolution.

Our CCSM training will enable you to develop complete mastery of Check Point R81.20 environments. You'll learn to manage distributed architectures, multi-site VPN scenarios, multi-datacenter high availability, automation via API and response to advanced attacks.

With a resolutely practical approach, you'll be able to design, administer and troubleshoot critical security infrastructures, while preparing for CCSM R81.20 certification.

This international certification is recognized as a real guarantee of mastery, and opens the way to the roles of security architect and SOC expert.

Like all our training courses, this one is based on the latest stable version of the Check Point ecosystem, with an emphasis on advanced hands-on training.

Objectives

- Design and administer complex Check Point environments.
- Optimize high availability and multi-site clustering scenarios.
- Deploy and secure advanced VPNs and hybrid architectures.
- Automate security via APIs and DevSecOps integrations.
- Carry out forensic investigations and advanced threat hunting.
- Pass CCSM R81.20 certification.

Target audience

- Senior security engineers
- Cybersecurity architects
- SOC managers
- IT security consultants

Prerequisites

- CCSE R81.x certification strongly recommended (or equivalent experience)
- Strong TCP/IP networking and cybersecurity skills
- Proven experience in the administration of Check Point solutions

CCSM Training Program

[Day 1 - Morning]

Introduction to CCSM and advanced reminders

- Presentation of CCSM certification and its positioning
- Prerequisites: mastery of CCSA/CCSE concepts
- CCSM R81.20 exam objectives and expectations
- Presentation of the advanced lab environment
- Practical workshop: Setting up the CCSM training lab.

[Day 1 - Afternoon]

Advanced policies and optimizations

- Managing complex policies and advanced rules
- Security segmentation and multiple domains
- Policy performance analysis
- Rule management automation
- Practical workshop: Optimizing a policy in a large environment.

Advanced authentication and access control

- Integration with SSO, SAML, MFA
- Identity and context-based access control
- Troubleshooting of hybrid environments
- Advanced authentication log management
- Practical workshop: MFA integration with an external IS.

[Day 2 - Morning]

Address translation and advanced routing

- Advanced NAT: complex scenarios and exceptions
- Dynamic routing and integration with BGP/OSPF
- Analysis of hybrid flows (cloud + on-prem)
- Advanced translation and routing troubleshooting
- Practical workshop: Implementing dynamic routing with complex NAT.

[Day 2 - Afternoon]

Monitoring and advanced observability

- Advanced logging and correlation
- SmartEvent and customized dashboards
- Integration with enterprise SIEM
- Proactive supervision and capacity planning
- Practical workshop: Creating a complete SOC dashboard.

Advanced VPNs and distributed architectures

- Advanced site-to-site VPNs (redundancy, multi-hubs)
- Remote Access VPN: scalability and hardening
- Complex IPSec VPN troubleshooting
- Hybrid cloud + on-prem security with VPN
- Practical workshop: Setting up a multi-site distributed VPN.

[Day 3 - Morning]

Advanced high availability

- ClusterXL: complex, multi-datacenter scenarios
- Multi-level synchronization and cluster troubleshooting
- Maintenance and non-disruptive upgrades
- Resilience strategies and disaster recovery
- Practical workshop: Incident simulation and distributed failover.

[Day 3 - Afternoon]

Advanced Threat

Prevention

- IPS/Anti-Bot/Threat Emulation optimization
- Full HTTPS inspection and constraints
- Signature performance and tuning
- Complex attack scenarios and response
- Practical workshop: Tuning and response to an APT scenario.

Automation and API

- Advanced use of the Check Point API
- Scripting and DevSecOps integration
- Automated management of rules and objects
- Security as Code and orchestration
- Practical workshop: Automating deployment via API.

[Day 4 - Morning]

Forensic and investigation

- Evidence gathering and advanced logging
- Check Point forensic tools
- Incident analysis and threat hunting
- Writing a post-incident report
- Practical workshop: Simulation of a SOC investigation.

[Day 4 - Afternoon]

Multi-domain and complex architectures

- Advanced concepts of Multi-Domain Security Management (MDM)
- Hybrid and multi-client scenarios
- Roles and permissions management
- Migration and business continuity
- Practical workshop: Complex multi-domain deployment.

Advanced troubleshooting

- Expert troubleshooting methodology
- Advanced tools: fw monitor, cpview, kernel debug
- Cluster, VPN, NAT and policy diagnostics
- Proactive detection of anomalies
- Practical workshop: Multi-layer incident resolution.

[Day 5 - Morning]

Cloud and hybrid security

- Integration with AWS, Azure and GCP
- Check Point CloudGuard and hybrid orchestration
- Native and hybrid cloud use cases
- Advanced security for cloud workloads
- Practical workshop: Securing a hybrid infrastructure.

[Day 5 - Afternoon]

Going live and sustainability

- Preparation and go-live checklist
- Advanced maintenance and upgrades
- Performance tuning and scalability
- FinOps best practices and governance
- Practical workshop: Simulated deployment and monitoring.

Preparation for CCSM certification

- Structure of the official CCSM R81.20 exam
- Key topics and weighting by domain
- Preparation strategy and final review
- Exam simulation and pitfalls to avoid
- Practical workshop: Passing the mock exam + correction.

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming training course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.