# Course : CCSE Check Point Certified Security Expert R82, certification

*Practical course - 4d - 28h00 - Ref. CPK*
*Price : 2890 CHF E.T.*

NEW

La formation enseigne l'usage des APIs, la gestion des politiques de sécurité, VPN et performances réseau. Elle couvre le déchiffrement HTTPS, SmartEvent, l'authentification, et la haute disponibilité avec ElasticXL La formation prépare à la certification CCSE.

## Teaching objectives

**At the end of the training, the participant will be able to:**

- ✓ Automate management via API
- ✓ Perform advanced upgrades
- ✓ Understanding Check Point internal processes and security policy installation
- ✓ Optimizing network performance
- ✓ Configuring Domain-Based VPNs with routing
- ✓ Implement secure remote access
- ✓ Supervise events and logs
- ✓ Decrypt HTTPS traffic. Understanding HTTP/3 protocol management
- ✓ Manage user authentication
- ✓ Mastering high availability and load balancing

## Intended audience

System/network/security technicians, administrators and engineers.

## Prerequisites

Good knowledge of TCP/IP, IS security and Check Point's main functions, or completion of the course "CCSA, Check Point Certified Security Administrator R82" (Ref. CPH).

### PARTICIPANTS

System/network/security technicians, administrators and engineers.

### PREREQUISITES

Good knowledge of TCP/IP, IS security and Check Point's main functions, or completion of the course "CCSA, Check Point Certified Security Administrator R82" (Ref. CPH).

### TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

### ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

## Practical details

### Exercise

Active, participative teaching through practical exercises.

## Course schedule

### 1 Advanced Gaia administration & API

- Using the Gaia CLI interface.
- Object and rule creation via API.
- Automation with REST API calls.

**Exercise**

Installation du SMS et des GWs en R81.20. Utilisation de l'API pour créer des objets et règles de base.

### 2 Check Point system upgrades

- Gaia update methods.
- Centralized upgrade of gateways and management servers.

**Exercise**

Mise à niveau avancée du Management de R81.20 vers R82. Mise à niveau centralisée de la passerelle principale et distante.

### 3 Check Point processes and security policy installation

- How Check Point processes work. Commands to view them
- Using SmartTasks with scripts for automation.
- Accelerated installation of the safety policy.
- Policy Packages, Layers, Updatable Objects.
- Introduction of Dynamic Layer, direct communication with gateway via API.

**Exercise**

Configure SmartTasks. Vérification des fichiers d'installation. Création des objets dynamiques. Utilisation du « Dynamic Layer » pour créer des objets et règles directement dans le firewall principal.

### 4 Optimizing performance - SecureXL & CoreXL

- Hardware and software acceleration.
- CoreXL Affinity, Dynamic Dispatcher, Hyperflow.

### 5 Advanced VPN - Domain-Based Routing

- Domain-Based vs Route-Based VPN.
- Tunnel monitoring with Network Probe.
- Wire Mode and authentication methods.

**Exercise**

Setting up VPN routing (Domain-Based).

**TEACHING AIDS AND TECHNICAL RESOURCES**

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.

• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.

• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

**TERMS AND DEADLINES**

Registration must be completed 24 hours before the start of the training.

**ACCESSIBILITY FOR PEOPLE WITH DISABILITIES**

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

### 6 Secure remote access

- SSL/IPSec VPN with Mobile Access Blade.
- SAML authentication and Active Directory integration.

**Exercise**
Setting up Remote Access and SSL VPN connections

### 7 Logs, monitoring and SmartEvent

- SmartEvent, SAM, ConnView.
- Advanced reporting and compliance.

**Exercise**
SmartEvent configuration.

### 8 HTTPS inspection and application security

- HTTPS, SNI, HTTP/3 (QUIC) decryption.
- Performance modes and certificate management.

**Exercise**
Implementation of HTTPS inspection.

### 9 User-based policy

- Identity Awareness, Access Roles.

**Exercise**
Authentication: implementation of Identity Awareness, creation of roles and accesses.

### 10 Clustering

- High availability and load sharing with ClusterXL and ElasticXL.

**Exercise**
Implementation of Load Sharing via ElasticXL.

## Options

**Certification : 300 € HT**

La certification est délivrée par Check Point Software Technologies. Elle valide les compétences avancées nécessaires pour administrer, optimiser et sécuriser les infrastructures Check Point. La durée est de 90 minutes et repose sur un QCM de 90 questions, en anglais.

The certification option comes in the form of a voucher or invitation that will allow you to take the exam at the end of the training course.

## Dates and locations

**REMOTE CLASS**
2026 : 31 Mar., 23 June, 6 Oct., 15 Dec.