

# Check Point Cyber Security Engineering (CCSE)

ID CCSE Preis auf Anfrage Dauer 3 Tage

## Zielgruppe

Der Kurs eignet sich für fortgeschrittene Nutzer und Reseller, die erweiterte Bereitstellungs-konfigurationen von Check Point Software Blades durchführen müssen.

## Empfohlenes Training für die Zertifizierung zum

Check Point Certified Security Expert (CCSE)

## Voraussetzungen

- Grundlagen in Unix-ähnlichen und/oder Windows-Betriebssystemen
- Kenntnisse in Netzwerktechnik, Netzwerksicherheit, Systemadministration und TCP/IP-Vernetzung
- Sicherer Umgang mit Texteditoren in Unix-ähnlichen Umgebungen
- Mindestens sechs Monate praktische Erfahrung mit Quantum Security
- Check Point Certified Security Administrator R82 (CCSA)-Ausbildung (obligatorisch)
- Check Point Deployment Administrator R82 (CPDA) (optional)

## Kursziele

Überprüfen Sie Ihr Verständnis und Ihre Fähigkeiten, um die Check Point Next Generation Firewalls zu konfigurieren und optimal zu verwalten.

## Kursinhalt

### Systemmanagement und Hochverfügbarkeit

- Verwaltung und Aktualisierung von Security Management Servern (inkl. Upgrades und Hotfixes).
- Einsatz von Management High Availability und Konfiguration sekundärer Server.
- Nutzung zentraler Deployment-Tools für effiziente Installationen.

### Richtlinien- und Gateway-Administration

- Fortgeschrittenes Policy Management.
- Konfiguration von Site-to-Site VPNs.
- Manuelle Network Address Translation.
- Verwaltung von Objekten mit der Check Point API.

### Cluster- und Performance-Technologien

- Einrichtung und Betrieb von ElasticXL- sowie ClusterXL-Clustern.
- Nutzung von SecureXL- und CoreXL-Technologien zur Leistungssteigerung.

### Automatisierung und Orchestrierung

- Einsatz flexibler Check Point API-Architekturen.
- Integration von Automatisierungs- und Orchestrierungslösungen in den Betrieb.

### Sicherheitsüberwachung und Bedrohungsmanagement

- Nutzung von SmartEvent zur Protokollauswertung, Ereigniserkennung und Bedrohungsanalyse.
- Überblick über IPS, Geo Protection, Threat Emulation und Threat Extraction.
- Prävention von Zero-Day-Angriffen und Advanced Persistent Threats.

### Mobil- und Remote-Sicherheit

- Mobile Access Software Blade: Bereitstellung, Verwaltung und Absicherung von Kommunikation und Daten.
- Remote-Access-Lösungen und Capsule-Komponenten für mobile Sicherheit.
- Schutz mobiler Geräte und Geschäftsdokumente mit Mobile Threat Prevention.

### Praktische Übungen

- Konfiguration von Security Gateway Clustern.
- Anwendung von Hotfixes und Updates.
- Arbeiten mit CLI-Befehlen und Modulen.
- Überprüfung und Feinjustierung von Threat-Prevention-Einstellungen.

# Check Point Cyber Security Engineering (CCSE)

---

## Weltweite Trainingscenter



## Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3  
CH-8304 Wallisellen  
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>