

## 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 Bereitstellungsconfigurationen von Check Point Software Blades durchführen müssen.

### Voraussetzungen

- CCSA Training/Zertifizierung
- Kenntnisse über Windows, UNIX, networking, TCP/IP, und Internet.

### Kursziele

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

### Kursinhalt

- Identifizieren Sie erweiterte CLI-Befehle
- Verstehen Sie Systemverwaltungsprozeduren, einschliesslich der Durchführung von System-Upgrades und Anwenden von Patches und Hotfixes.
- Beschreiben Sie die Check Point Firewall-Infrastruktur
- Beschreiben Sie erweiterte Methoden zum Sammeln wichtiger Gateway-Daten mit CPView und CPInfo
- Erkennen Sie, wie die flexible API-Architektur von Check Point die Automatisierung und die Orchestrierung unterstützt
- Besprechen Sie die erweiterten ClusterXL-Funktionen
- Beschreiben von VRRP-Netzwerk-Redundanzvorteilen. Untersuchen Sie, wie die SecureXL Beschleunigungstechnologie verwendet wird, um die Leistung zu verbessern und zu verbessern
- Beschreiben von VRRP-Netzwerk-Redundanzvorteilen
- Verstehen Sie, wie die SecureXL Beschleunigungstechnologie verwendet wird, um die Leistung zu verbessern und zu verbessern.
- Verstehen Sie, wie die CoreXL-Beschleunigungstechnologie verwendet wird, um die Leistung zu verbessern und zu verbessern

- Identifizieren Sie die SmartEvent-Komponenten, die Netzwerkaktivitätsprotokolle speichern und Ereignisse erkennen
- Besprechen Sie den SmartEvent-Prozess, der festlegt, welche Netzwerkaktivitäten zu Sicherheitsfragen führen können
- Verstehen Sie, wie SmartEvent bei der Erkennung, Abhilfe und Vermeidung von Sicherheitsbedrohungen helfen kann
- Diskutieren Sie die Mobile Access Software Blade und wie sich die Kommunikation und Daten sicherstellt
- Verstehen Sie die Möglichkeiten zur Bereitstellung von Mobilgeräten
- Erkennung von Check Point Remote Access Lösungen
- Diskutieren Sie Check Point Capsule-Komponenten und wie sie mobile Geräte und Geschäftsdokumente schützen
- Diskutieren Sie verschiedene Check Point-Lösungen für Angriffe wie z. B. Zero-Day und Advanced Persistent Threats
- Verstehen Sie, wie SandBlast, Threat Emulation und Threat Extraction Sicherheitsvorfälle verhindern
- Identifizieren Sie, wie Check Point Mobile Threat Prevention zum Schutz von Daten, die auf von Unternehmen ausgegebene Smartphones und Tablets zugegriffen werden, helfen kann

# Check Point Cyber Security Engineering (CCSE)

---

## Weltweite Trainingscenter



## Fast Lane Institute for Knowledge Transfer GmbH

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

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