

Mit Hilfe der Software-Blade-Architektur von Check Point lassen sich leicht individuell angepasste Netzwerk Security-Lösungen (Firewall) implementieren.

**Ihr Nutzen**

In diesem Kurs wird das Wissen vertieft und Methoden zum Debuggen und Troubleshooting vorgestellt. Die Teilnehmer haben in der Testnetzumgebung die Möglichkeit, das Erlernete umzusetzen und selbstständig Probleme zu lösen.

**Preis pro Teilnehmer**

EUR 2195,- exklusive der gesetzlichen MwSt.

**Seminardauer**

3 Tag(e)/Day(s)

**Seminarinhalte****1. Tag**

- \* Systemmanagement
- Aktualisieren eines Security Management Servers auf R80.10
- Anwenden von Check Point-Hotfixes
- \* Automatisierung und Orchestrierung
- Wichtige CLI-Elemente der Firewall-Administration
- Konfigurieren von manueller Network Address Translation
- Verwalten von Objekten mit der Check Point-API
- \* Redundanz
- Konfigurieren eines neuen Security Gateway Clusters
- Bereitstellen eines sekundären Security Management Servers

**2. Tag**

- \* Beschleunigen
- Aktivierung von Check Point VRRP
- Anzeigen der Chain-Module
- Arbeiten mit SecureXL
- Arbeiten mit CoreXL
- \* SmartEvent
- Auswertung von Bedrohungen mit SmartEvent

**3. Tag**

- \* Mobil- und Remote-Zugriff
- Verwalten von Mobile Access
- \* Schutz vor Bedrohungen
- Überblick über IPS Protection
- Bereitstellung von IPS Geo Protection
- Überprüfung der Threat-Prevention-Einstellungen
- Bereitstellung von Threat Emulation und Threat Extraction

**Voraussetzungen**

Check Point Security Administration~8933  
oder dem entsprechende Kenntnisse

Grundlegende Netzwerk und IPV4 / IPV6 Kenntnisse. Grundlagen in Windows und Unix und mit Netzwerkdiensten.

**Hinweise**

CCSE\_R81.20, Dieses Seminar wird mit einem zertifizierten Trainingspartner durch geführt und dient somit auch als Vorbereitung für Ihre Zertifizierung. Die Prüfungsgebühr von 250,00 € ist im Kurspreis nicht enthalten.

Version: R81

