Check Point Cybersecurity BootCamp R81.20

CCSA & CCSE

Check Point Cybersecurity BootCamp R81.20

Die Zertifizierung zum CCSA R81.20 und CCSE R81.20 erfordert normalerweise den Besuch von zwei dreitägigen Kursen. Für Teilnehmer, die schon umfangreiche Erfahrungen mit der Check Point Firewall vorweisen können und vielleicht schon eine frühere Zertifizierung zum CCSA/CCSE abgeschlossen haben, bietet sich dieses BootCamp an.

Um schneller ans Ziel der Zertifizierung zu kommen, werden in diesem fünftägigen BootCamp alle prüfungsrelevanten Inhalte und Laborübungen der beiden Kurse Check Point Certified Security Administrator R81.20 – CCSA und Check Point Certified Security Expert R81.20 – CCSE in konzentrierter Form erarbeitet. Die erweiterten Kurszeiten (täglich von 8-18 Uhr) bilden den zeitlichen Rahmen für den Kurs. Für Nachbereitung und Selbststudium der Inhalte steht den Teilnehmern innerhalb der Kurswoche zusätzlich das Labor rund um die Uhr zur Verfügung. Am Ende des Kurses haben die Teilnehmer das Wissen, um die Examen zum CCSA und CCSE R81.20 abzulegen. Das Ablegen der Examen ist nicht Bestandteil dieses BootCamps.

Kursinhalt
CCSA - Security Administrator

- Security Management
- SmartConsole
- Deployment
- Object Management
- Licenses and Contracts
- Policy Rules and Rulebase
- Policy Packages
- Policy Layers
- Traffic Inspection
- Network Address Translation
- Application Control
- URL Filtering
- Logging
- Snapshots
- Backup and Restore
- Gaia
- Permissions
- Policy Installation

CCSE - Security Expert

- Advanced Deployments
- Management High Availability
- Advanced Gateway Deployment
- Advanced Policy Configuration
- Advanced User Access Management
- Custom Threat Protection
- Advanced Site-to-Site VPN
- Remote Access VPN
- Mobile Access VPN
- Advanced Security Monitoring
- Performance Tuning
- Advanced Security Maintenance

E-Book Sie erhalten die englischen Original-Unterlagen als Check Point e-Kit.

Zielgruppe
Dieser Kurs richtet sich an Teilnehmer, die Erfahrung in der Arbeit mit Check Point Firewalls besitzen und das Wissen aus den Kursen CCSA R81.20 und CCSE R81.20 in kompakter Form erlernen möchten

Voraussetzungen
Ein Jahr Erfahrung mit Check Point Produkten. Arbeitskenntnisse in Windows, UNIX, Netzwerktechnologie, Internet und TCP/IP werden empfohlen.

Kursziel
CCSA - Security Administrator

- Beschreiben Sie die Hauptkomponenten einer dreistufigen Check Point-Architektur und erklären Sie, wie sie in der Check Point-Umgebung zusammenarbeiten.
- Identifizieren Sie den grundlegenden Arbeitsablauf für die Installation des Security Management Servers und des Security Gateways für eine Single-Domain-Lösung.
- Erstellen Sie SmartConsole-Objekte, die der Topologie des Unternehmens entsprechen, zur Verwendung in Richtlinien und Regeln.
- Identifizieren Sie die verfügbaren Tools zur Verwaltung von Check Point Lizenzen und Verträgen, einschließlich ihres Zwecks und ihrer Verwendung.
- Identifizieren Sie Features und Funktionen, die die Konfiguration und Verwaltung der Sicherheitsrichtlinien verbessern.
- Demonstrieren Sie Ihr Verständniss von Application Control & URL Filtering und Autonomous Threat Prevention und wie man diese Lösungen konfiguriert, um die Sicherheitsanforderungen einer Organisation zu erfüllen.
- Beschreiben Sie, wie man den VPN-Tunnelverkehr analysiert und interpretiert.
- Beschreiben Sie, wie man den Zustand der unterstützten Check Point Hardware mit Hilfe des Gaia Portals und der Kommandozeile überwacht.
- Beschreiben Sie die verschiedenen Methoden zur Sicherung von Check Point Systeminformationen und diskutieren Sie Best Practices und Empfehlungen für jede Methode.

CCSE - Security Expert

- Identifizieren Sie die Arten von Technologien, die Check Point für die Automatisierung unterstützt.
- Erklären Sie den Zweck der Check Management High Availability (HA) Bereitstellung.
- Erklären Sie die grundlegenden Konzepte von Clustering und ClusterXL, einschließlich Protokollen, Synchronisation und Verbindungsstabilität.
- Erläutern Sie den Zweck von dynamischen Objekten, aktualisierbaren Objekten und Netzwerk-Feeds.
- Beschreiben Sie die Komponenten und Konfigurationen von Identity Awareness.
- Beschreiben Sie die verschiedenen Check Point Threat Prevention Lösungen.
- Erläutern Sie, wie das Intrusion Prevention System konfiguriert wird.
- Erläutern Sie den Zweck von domänenbasierten VPNs.
- Beschreiben Sie Situationen, in denen eine extern verwaltete Zertifikatsauthentifizierung verwendet wird.
- Beschreiben Sie, wie die Client-Sicherheit durch Remote Access gewährleistet werden kann.
- Erläutern Sie die Mobile Access Software Blade.
- Definieren Sie Lösungen zur Leistungsoptimierung und grundlegende Konfigurationsabläufe.
- Identifizieren Sie unterstützte Upgrade-Methoden und -Verfahren für Security Gateways.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/**CPB8**

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.
Termine in Deutschland	**5 TageCHF 3.955,-**
Online Training	**5 TageCHF 3.955,-**
Termin/Kursort	Kurssprache Deutsch
10.11.-14.11.25 Frankfurt	10.11.-14.11.25 Online

Stand 16.04.2025

Check Point

ExperTeach

Inhaltsverzeichnis

Check Point Cybersecurity BootCamp R81.20 – CCSA & CCSE

Übungen

CCSA - Security Administrator
Deploy SmartConsole
Install a Security Management Server
Install a Security Gateway
Configure Objects in SmartConsole
Establish Secure Internal Communication
Manage Administrator Access
Manage Licenses
Create a Security Policy
Configure Order Layers
Configure a Shared Inline Layer
Configure NAT
Integrate Security with a Unified Policy
Elevate Security with Autonomous Threat Prevention
Configure a Locally Managed Site-to-Site VPN
Elevate Traffic View
Monitor System States
Maintain the Security Environment

CCSE - Security Expert
Navigate the Environment and Use the Management API
Deploy Secondary Security Management Server
Configure a Dedicated Log Server
Deploy SmartEvent
Configure a High Availability Security Gateway Cluster
Work with ClusterXL
Configure Dynamic and Updateable Objects
Verify Accelerated Policy Installation and Monitoring Status
Elevate Security with HTTPS Inspection
Deploy Identity Awareness
Customize Threat Prevention
Configure a Site-to-Site VPN with an Interoperable Device
Deploy Remote Access VPN
Configure Mobile Access VPN
Monitor Policy Compliance
Report SmartEvent Statistics
Tune Security Gateway Performance