Maslak Mahallesi, Maslak Meydan Sk. No:5. Spring Giz Plaza. Maslak/İstanbul
+90 212 282 7700 - info@bilginc.com

# Check Point Cyber Security Engineering (CCSE) R80.20

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **3 Gün**

## Overview

Check Point Cyber Security Engineering R80.20, Check Point Yeni Nesil Güvenlik Duvarlarının etkin bir şekilde nasıl yapılandırılıp yönetileceğini öğreten, 3 günlük bir ileri düzey eğitimdir.

**Sınav Bilgileri**

Her ne kadar bu eğitim, Check Point CCSE sınavının hedeflerinin birçoğu ile uyumlu olsa da adaylar pratik konusunda deneyimli olmalı ve ayrıca sertifikasyona tamamen hazır olmak için de kendi kendine çalışma yöntemlerini benimsemelidir.

## Prerequisites

- CCSA R80.20 training/certification
- Working knowledge of Windows, UNIX, networking, TCP/IP, and the Internet.

## Who Should Attend

Bu eğitim, Check Point Yazılım Uçlarının ileri düzey kurulum yapılandırmalarını yapması gereken uzman kullanıcılar ve bayiler için tasarlanmıştır.

Bunlar arasında şu kişiler yer alabilir:

- Sistem Yöneticileri
- Destek Analistleri

## What You Will Learn

- Identify advanced CLI commands.
- Understand system management procedures, including how to perform system upgrades and apply patches and hotfixes.
- Describe the Check Point Firewall infrastructure.
- Describe advanced methods of gathering important gateway data using CPView and CPInfo.
- Recognize how Check Point's flexible API architecture supports automation and orchestration.
- Discuss advanced ClusterXL functions.
- Describe VRRP network redundancy advantages.
- Undersand how SecureXL acceleration technology is used to enhance and improve performance.
- Understand how CoreXL acceleration technology is used to enhance and improve performance.
- Identify the SmartEvent components that store network activity logs and identify events.
- Discuss the SmartEvent process that determines which network activities may lead to security issues.
- Understand how SmartEvent can assist in detecting, remediating, and preventing security threats.
- Discuss the Mobile Access Software Blace and how it secures communication and data.
- Understand Mobile Access deployment options.
- Recognize Check Point Remote Access solutions.
- Discuss Check Point Capsule components and how they protect mobile devices and business documents.
- Discuss diferent Check Point Solutions for attacks such as zero-day and Advanced Persistent Threats.
- Understand how SandBlast, Threat Emulation, and Threat Extraction prevent security incidents.
- Identify how Check Point Mobile Threat Prevention can help protect data accessed on company-issued smartphones and tablets.

## Outline

COURSE TOPICS

- System Management
- Automation and Orchestration
- Redundancy
- Acceleration
- SmartEvent
- Mobile and Remote Access
- Threat Prevention

LAB EXERCISES

- Upgrading a Security Management Server to R80.20
- Applying Check Point Hotfixes
- Configuring a New Security Gateway Cluster
- Core CLI Elements of Firewall Administration
- Configuring Manual Network Address Translation
- Managing Objects Using the Check Point API
- Enabling Check Point VRRP
- Deploying a Secondary Security Management Server
- Viewing the Chain Modules
- Working with SecureXL
- Working with CoreXL
- Evaluating Threats with SmartEvent
- Managing Mobile Access
- Understanding IPS Protections
- Deploying IPS Geo Protection
- Reviewing Threat Prevention Settings and Protections
- Deploying Threat Emulation and Threat Extraction