

# Check Point Cyber Security Administrator (CCSA) and Engineering Fast Track (CCSE) R80.20

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

Duration: **5 Gün**

## **Overview**

Bu 5 günlük hızlandırılmış eğitim hem Check Point Cyber Security Administration R80.20 hem de Check Point Cyber Security Engineering R80.20 eğitimlerini kapsayacaktır.

Bu eğitimler, Check Point Güvenlik Ağ Geçidini ve Yönetim Yazılımını yapılandırmak için gereken temel kavramları ve becerileri kavramanızı sağlayacaktır. Eğitim sırasında bir Güvenlik Politikası'nı yapılandırarak ve güvenli bir ağı yönetmeyi ve izlemeyi, bir Güvenlik Ağ Geçidi'ni yükseltmeyi ve yapılandırmayı ve bir sanal özel ağı uygulamaya koymayı öğreneceksiniz. Eğitim ayrıca Check Point Güvenlik sistemlerini etkin bir şekilde nasıl oluşturacağınızı, değiştireceğinizi, kuracağınızı ve sorunlarını tespit edip gidereceğinizi de kapsayacaktır. Güvenlik duvarı süreçlerini çalışacağız ve kullanıcı ve kernel işleme ile Durum Denetimine yakından bakacağız. Laboratuvarlar arasında ise güvenlik ağ geçitlerinin yapılandırılması, VPN'lerin uygulamaya konulması, güvenlik duvarı üzerinde gelişmiş sorun tespit ve giderme işlerinin yürütülmesi yer almaktadır.

## **Sınav Bilgileri**

Her ne kadar bu eğitim, Check Point CCSA ve CCSE sınavlarının 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**

Persons attending this course should have general knowledge of TCP/IP, and working knowledge of Windows, UNIX, network technology and the internet

## **Who Should Attend**

Check Point Yazılım Uçlarını destekleyen, yükleyen, kuran veya yöneten teknik kişiler bu eğitime katılmalıdır. Bunlar arasında şu kişiler yer alabilir:

- Sistem Yöneticileri
- Destek Analistleri
- Güvenlik Yöneticileri
- Ağ Mühendisleri
- CCSA ve CCSE sertifikasyonuna sahip olmak isteyen herkes

## **What You Will Learn**

CCSA Topics

- Interpret the concept of a Firewall and understand the mechanisms used for controlling network traffic.
- Describe the key elements of Check Point's unified Security Management Architecture.
- Recognize SmartConsole features, functions and tools.
- Understand Check Point deployment options.
- Describe the basic functions of Gaia.
- Describe the essential elements of a Security Policy.
- Understand how traffic inspection takes place in a unified Security Policy.
- Summarize how administration roles and permissions assist in managing policy.
- Recall how to implement backup techniques.
- Understand the Check Point policy layer concept.

- Recognize Check Point security solutions and products and how they work to protect your network.
- Understand licensing and contract requirements for Check Point security products.
- Identify tools designed to monitor data, determine threats and recognize performance improvements.
- Identify tools designed to respond quickly and efficiently to changes in gateways, tunnels, remote users, traffic flow patterns, and other activities.
- Understand Site-to-Site and Remote Access VPN deployments and communities.
- Understand how to analyze and interpret VPN traffic.
- Recognize how to define users and user groups.
- Understand how to manage user access for internal and external users.
- Understand the basic concepts of ClusterXL technology and its advantages.
- Understand how to perform periodic administrator tasks as specified in administrator job descriptions.

#### CCSE Topics

- 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.
- Understand 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 Blade 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 different 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**

##### CCSA Course Exercises

- Introduction to Check Point Technology
- Security Policy Management
- Policy Layers
- Check Point Security Solutions and Licensing
- Traffic Visibility
- Basic Concepts of VPN
- Managing User Access
- Working with ClusterXL
- Administrator Task Implementation

##### Lab Exercises

- Working with Gaia Portal
- Modifying an Existing Security Policy
- Configuring Hide and Static NAT
- Managing Administrator Access
- Installing and Managing a Remote Security Gateway
- Managing Backups
- Defining Access Control Policy Layers
- Defining and Sharing Security Policy Layers
- Working with Licenses and Contracts
- Working with Check Point Logs
- Maintaining Check Point Logs
- Configuring a Site-to-Site VPN
- Providing User Access
- Working with Cluster XL
- Verifying Network Compliance
- Working with CP View

##### CCSE Course Exercises

- 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