# Check Point Cybersecurity Boot Camp (CCSA+CCSE) Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Overview

**New - Learn basic concepts and develop skills necessary to administer Check Point Next Generation Firewalls. Validate your understanding and skills necessary to configure and optimally manage Check Point Next Generation Firewalls.**

In this five-day bundle course, you will learn the basic concepts and skills necessary to configure Check Point Next Generation Firewalls. During this course, you will configure a security policy and learn about managing and monitoring a secure network, upgrading and configuring a security gateway, and implementing a virtual private network (VPN). You will also learn the advanced concepts and skills necessary to configure Check Point Next Generation Firewalls. During this course, you will configure a security policy and learn about managing and monitoring a secure network, upgrading and configuring a security gateway, and implementing a virtual private network (VPN).

**Note:** Supported versions R81.10 and previous versions

**Is This The Right Course?**

- General knowledge of TCP/IP
- Working knowledge of Windows, UNIX, network technology, and the internet

**Who Should Attend?**

Technical persons who support, install, deploy, or administer Check Point Software Blades, which includes:

- System administrators
- Support analysts
- Security managers
- Network engineers
- Anyone seeking CCSA certification and CCSE certification

## Prerequisites

- General knowledge of TCP/IP
- Working knowledge of Windows, UNIX, network technology, and the internet

# Check Point Cybersecurity Boot Camp (CCSA+CCSE) Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## What You Will Learn

- Security Architecture
- Application Control
- Deployment
- Licensing
- Gaia Portal
- Hide/Static NAT
- URL Filtering
- Monitoring States
- IoT
- Traffic Visibility
- Security Events
- Threat Extraction
- Threat Emulation
- Policy Layers
- Browser SmartConsole
- Infinity Threat Protection
- User Access
- System Management
- Automation and Orchestration
- Redundancy
- Acceleration
- SmartEvent
- Mobile and Remote Access
- Threat Prevention

## Outline

- Know how to perform periodic administrator tasks.
- Describe the basic functions of the Gaia operating system.
- Recognize SmartConsole features, functions, and tools.
- Understand how SmartConsole is used by administrators to give user access.
- Learn how Check Point security solutions and products work and how they protect networks.
- Understand licensing and contract requirements for Check Point security products.
- Describe the essential elements of a Security Policy.
- Understand the Check Point policy layer concept.
- Understand how to enable the Application Control and URL Filtering software.
- Blades to block access to various applications.
- Describe how to configure manual and automatic NAT.
- Identify tools designed to monitor data, determine threats and recognize opportunities for performance improvements.
- Describe different Check Point Threat Prevention solutions for network attacks.
- Articulate how the Intrusion Prevention System is configured, maintained and tuned.
- Understand the Infinity Threat Prevention system.
- Knowledge about Check Point’s IoT Protect.
- Provide an overview of the upgrade service and options available.
- Explain how to perform management upgrade and migration.
- Articulate the process using CPUSE features.
- Articulate the purpose and function of Management High Availability.

# Check Point Cybersecurity Boot Camp (CCSA+CCSE) Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Explain Primary vs Secondary, Active vs Standby and Synchronization.
- Explain disaster recovery steps in case the primary management server becomes unavailable.
- Provide overview of Central Deployment in SmartConsole.
- Articulate an understanding of Security Gateway cluster upgrade methods.
- Explain about Multi Version Cluster (MVC) upgrades.
- Discuss Gaia Commands and how they are used.
- Explain the main processes on s and s.
- Describe how to work with scripts and SmartTasks to configure automatic actions.
- Explain the Management Data Plane Separation (MDPS)
- Explain kernel operations and traffic flow
- Articulate Dynamic and Updatable Objects in Security Gateways
- Explain the policy installation flow and files used.
- Describe the use of policy installation history.
- Explain concurrent and accelerated install policy.
- Describe an overview of APIs and ways to use and authenticate.
- Explain how to make changes in GAIA and management configuration.
- Explain how to install policy using API.
- Explain how the SecureXL acceleration technology enhances and optimizes Security Gateway performance.
- Describe how the CoreXL acceleration technology enhances and improves Security Gateway performance.
- Articulate how utilizing multiple traffic queues can make traffic handling more efficient.
- Discuss Site-to-Site VPN basics, deployment and communities.
- Describe how to analyze and interpret VPN tunnel traffic.
- Explain Link Selection and ISP Redundancy options.
- Explain tunnel management features.
- Discuss Check Point Remote Access solutions and how they differ from each other.
- Describe how client security can be provided by Remote Access .
- Explain authentication methods including machine authentication.
- Explain Multiple Entry Point (MEP)
- Discuss the Mobile Access Software Blade and how it secures communication and data exchange during remote connections.
- Describe Mobile Access deployment options.
- Discuss various features in Mobile Access like Portals, Link Translation, running Native Applications, Reverse Proxy and more.
- Explain basic concepts of Clustering and ClusterXL.
- Explain about Cluster Control Protocol (CCP) and synchronization.
- Describe advanced ClusterXL functions and modes like Load Sharing, Active-Active, VMAC mode etc.
- Discuss Cluster Correction Layer (CCL) to provide connection stickyness.
- Advanced Logs and Monitoring