# Check Point Security Engineering (CCSE) Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Overview

The Check Point Security Engineering (CCSE) course provides advanced knowledge and practical experience for deploying, managing and monitoring complex **Check Point Quantum Security Environments**.

Building on core Check Point administration skills, the course moves participants into more advanced operational areas such as high availability, advanced policy configuration, secure connectivity across distributed environments, upgrades, migrations and clustering.

Throughout the programme, learners gain hands-on experience with **Management High Availability**, dynamic and advanced policy elements, manual NAT configuration, site-to-site VPNs, SmartEvent, the Compliance Blade, gateway and management server upgrades, database migration and **ElasticXL Cluster** deployment.

Guided laboratories and structured walkthroughs help participants deepen their operational capability and develop the expertise required to maintain resilient, scalable and high-performing Check Point security environments.

## Prerequisites

Participants should have:

- Experience working with Unix-like and Windows operating systems
- Knowledge of internet fundamentals
- Understanding of networking and network security
- System administration experience
- TCP/IP networking skills
- Familiarity with text editors in Unix-like environments
- At least six months of hands-on experience managing a Quantum Security Environment

**Required preparation:** Knowledge equivalent to Check Point Certified Security Administrator level.

## Who Should Attend

This course is particularly suitable for:

- Security engineers
- Security analysts
- Security consultants
- Security architects

The course content also aligns with NIST/NICE work role categories related to **Implementation and Operation** and **Protection and Defence**.

# Check Point Security Engineering (CCSE) Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## What You Will Learn

By the end of the course, participants will be able to:

- Deploy and configure Management High Availability to strengthen resilience and continuity
- Improve security policies through advanced object types, dynamic objects and manually defined NAT rules
- Configure and validate management behind NAT in distributed environments
- Build, analyse and manage site-to-site VPNs using internally managed gateways and advanced authentication options
- Interpret VPN tunnel traffic and apply link selection, ISP redundancy and tunnel management functionality
- Use advanced monitoring tools such as SmartEvent and the Compliance Blade to analyse events, alerts, patterns and compliance information
- Upgrade security gateways and deploy hotfixes with the Central Deployment tool
- Perform advanced management server upgrades and database migrations in distributed environments
- Deploy and configure ElasticXL Cluster solutions to improve scalability and high availability
- Validate operational performance and security posture through hands-on labs and practical scenarios

## Outline

### Management High Availability

This section introduces the purpose, architecture and deployment considerations associated with management-level high availability.

- Purpose of Management High Availability
- Key components
- Deployment considerations

### Lab Activities

- Deploy Management High Availability
- Configure high availability settings
- Validate failover behaviour
- Test high availability functions

### Advanced Policy Management

This section focuses on advanced configuration options that can make security policies more flexible and dynamic.

- Enhancing security policies with advanced object types
- Creating dynamic objects for gateway-updatable policies
- Manually defining NAT rules
- Configuring management behind NAT in distributed environments

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


### Lab Activities

- Use updatable objects
- Configure NAT for server objects
- Configure NAT for network objects
- Configure management behind NAT for branch office connectivity

### Site-to-Site VPN

Participants explore secure connectivity between distributed networks using site-to-site VPN technologies.

- Site-to-site VPN concepts and deployment models
- VPN communities
- VPN traffic flow analysis
- Pre-shared key authentication
- Certificate-based authentication
- Link selection
- ISP redundancy
- Tunnel management behaviour

### Lab Activity

- Configure a site-to-site VPN using internally managed security gateways

### Advanced Security Monitoring

This section examines tools used to analyse security activity, events, alerts and compliance information in greater depth.

- Purpose and capabilities of SmartEvent
- Compliance Blade functionality
- Event analysis
- Alert configuration
- Pattern monitoring
- Compliance reporting

### Lab Activities

- Configure a SmartEvent Server
- Configure events and alerts
- Run SmartEvent reports
- Activate the Compliance Blade
- Review best-practice settings and alerts
- Validate regulatory compliance scoring

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


## Upgrades

Participants examine supported methods and workflows for upgrading Check Point components.

- Supported upgrade methods
- Upgrade workflows and considerations

## Lab Activities

- Upgrade a security gateway
- Use the Central Deployment tool to install hotfixes

## Advanced Upgrades and Migrations

This section focuses on management server upgrades and database migration processes.

- Exporting a management database
- Importing a management database
- Upgrading a management server by deploying a new release or appliance

## Lab Activities

- Prepare for an advanced upgrade with database migration in a distributed environment
- Perform an import of a primary Security Management Server

## ElasticXL Cluster

Participants examine ElasticXL Cluster architecture and its use for improving scalability and high availability.

- Purpose of ElasticXL Cluster
- Design approach
- Deployment considerations
- Operational behaviour

## Lab Activity

- Deploy an ElasticXL Security Gateway Cluster

## Exams and Assessments

This course is designed to prepare participants for **Certification Exam 156-315.82**.

No formal certification examination is delivered as part of the course itself. Instead, participants complete:

- Practical lab tasks

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- Structured exercises
- Realistic operational scenarios

to reinforce advanced administration skills and validate practical capability.

### Hands-On Learning

A significant portion of the course is delivered through advanced hands-on laboratories. Participants work through realistic tasks across:

- High Availability management
- Advanced policy configuration
- NAT
- Site-to-site VPN
- SmartEvent
- Compliance Blade
- Gateway upgrades
- Hotfix deployment
- Management server migration
- Database migration
- ElasticXL Cluster deployment

Instructors support participants throughout the exercises with configuration guidance, troubleshooting assistance, validation and advanced operational insights.