Check Point Security Administration (CCSA) Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The Check Point Security Administration (CCSA) course introduces the key concepts, tools and administrative processes required to configure, manage and monitor a **Check Point Quantum Security Environment**.

Throughout the course, participants gain practical experience with the **Gaia Portal**, **Gaia Command Line Interface**, **SmartConsole** and the Check Point three-tier architecture. The programme covers a broad range of administration and security topics, including object management, security policy configuration, ordered and inline layers, HTTPS Inspection, Identity Awareness, Application Control, URL Filtering and Autonomous Threat Prevention.

Through guided laboratories and realistic configuration scenarios, learners develop the practical confidence required to secure, optimise, monitor and maintain a Quantum deployment.

Prerequisites

Participants should have a working knowledge of:

- Unix-like and Windows operating systems
- Internet fundamentals
- Networking concepts
- Network security principles
- System administration
- TCP/IP networking

Who Should Attend

This course is particularly suitable for:

- Security administrators
- 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 Administration (CCSA) Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

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

- Explain the Check Point three-tier architecture and its function within a Quantum Security Environment
- Work effectively with the Gaia Portal, Gaia CLI and core SmartConsole views
- Create and manage administrator accounts, permission profiles and collaborative session controls
- Configure physical and logical objects in SmartConsole to support security policy design
- Create, modify and validate security policies based on organisational access requirements
- Implement and test ordered and inline policy layers to improve traffic inspection
- Monitor platform performance, logs, events and system state using SmartConsole and Gaia tools
- Configure Identity Awareness components and incorporate user identity into policy rules
- Enable and tune HTTPS Inspection to improve visibility of encrypted traffic
- Apply Application Control and URL Filtering to manage application and web access
- Enable and validate Autonomous Threat Prevention to strengthen the overall security posture

Outline

Introduction to Quantum Security

This section introduces the core architecture and administration tools used within a Check Point Quantum environment.

- Overview of the Check Point three-tier architecture
- Interaction between management servers, log servers and gateways
- Navigation of key SmartConsole views
- Accessing and reviewing Gaia on management servers, log servers and gateway clusters

Lab Activities

- Explore Gaia on management, log and gateway systems
- Connect to SmartConsole
- Navigate Gateways & Servers
- Review Security Policies
- Work with Logs & Events
- Explore Manage & Settings

Administrator Account Management

This section examines the purpose of SmartConsole administrator accounts and the options available for controlling administrative access.

- Purpose of SmartConsole administrator accounts
- Session management
- Concurrent administration capabilities
- Administrator profile assignment

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Lab Activities

- Create administrator accounts and assign profiles
- Test administrator permissions and session controls
- Manage concurrent administrative sessions
- Take over another administrator session

Object Management

Participants explore how SmartConsole objects are used to represent infrastructure and services within security policies.

- Purpose and function of SmartConsole objects
- Physical and logical object types
- Use of objects within policy operations

Lab Activities

- View and modify gateway and server objects
- Manage network objects
- View and update service objects

Security Policy Management

This section focuses on creating and maintaining policies that control network access and security behaviour.

- Purpose of security policies
- Core components of a policy rule
- Features that support efficient policy configuration and management

Lab Activities

- Verify the existing security policy
- Modify policy rules
- Install the standard policy
- Test policy rule outcomes

Policy Layers

Participants examine how multiple policy layers can be used to structure and refine traffic inspection.

- Concept and purpose of ordered policy layers
- Effect of layers on traffic inspection
- Creation of inline layers such as a DMZ layer

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Lab Activities

- Add an ordered layer
- Configure and deploy ordered layer rules
- Test ordered layer behaviour
- Create an inline DMZ layer
- Validate inline layer results

Security Operations Monitoring

This section explores the tools and techniques used to monitor activity and platform health in a Check Point environment.

- Purpose of monitoring
- Log server configuration and optimisation
- Querying and filtering log information
- Monitoring system state and blade status

Lab Activities

- Configure log management settings
- Improve rulebase views and logging behaviour
- Review logs and perform targeted searches
- Configure the Monitoring Blade
- Monitor system status

Identity Awareness

Participants learn how user identity can be incorporated into policy decisions.

- Purpose and function of Identity Awareness
- Core components and identity sources
- Integrating identity into security policies

Lab Activities

- Modify the security policy for Identity Awareness
- Configure the Identity Collector
- Define user access roles
- Test identity-based access

HTTPS Inspection

This section covers the inspection of encrypted HTTPS traffic for security purposes.

- Purpose of HTTPS Inspection
- Core components

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Key configuration concepts

Lab Activities

- Enable HTTPS Inspection
- Modify Access Control rules
- Deploy the gateway certificate
- Test and analyse policy behaviour with inspection enabled

Application Control and URL Filtering

Participants learn how Check Point features can be used to manage access to applications and web resources.

- Purpose of Application Control
- Purpose of URL Filtering
- Core configuration workflow

Lab Activities

- Modify the Access Control Policy
- Create Application and URL Filtering rules
- Update existing rules
- Test and refine rule behaviour

Threat Prevention Fundamentals

This section introduces Check Point threat prevention capabilities.

- Purpose of Autonomous Threat Prevention
- Main components of the Threat Prevention solution

Lab Activities

- Enable Autonomous Threat Prevention
- Test and validate threat prevention behaviour

Exams and Assessments

This course is designed to prepare participants for **Exam 156-215.82**.

No formal certification assessment is included within the training delivery itself. Instead, participants complete a combination of:

- Structured lab activities
- Knowledge checks
- Practical validation exercises

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

throughout the programme to reinforce both understanding and practical competence.

Hands-On Learning

A significant part of the course is delivered through practical laboratory activities. Participants work directly with Check Point technologies and gain hands-on experience in:

- Gaia administration
- SmartConsole
- Security policy management
- Identity Awareness
- HTTPS Inspection
- Application Control
- URL Filtering
- Autonomous Threat Prevention
- Logging and system monitoring

Instructors support participants throughout the exercises with configuration guidance, troubleshooting and validation of completed tasks.