

# Cybersecurity Boot Camp R81.10 (CCSA-CCSE)

Kód kurzu: CCSACCSE

This 5-day Boot Camp course combines the content of the CCSA and CCSE courses. This course is not for new users to Check Point – previous certification/experience is required. Check Point Certified Security Administrator (CCSA) - The CCSA part of the course covers everything you need to start-up, configure and manage daily operations of R81.10 Check Point Security Gateway and Management Software Blades systems on the GAiA operating system. Goals: Learn basic concepts and develop skills necessary to administer IT security fundamental tasks. Topics: Security Architecture, Application Control, Deployment, Licensing, Gaia Portal, Hide/Static NAT, URL Filtering, Monitoring States, IoT, Traffic Visibility, Security Events, Threat Emulation, Policy Layers, Browser SmartConsole, Infinity Threat Prevention, User Access.

Check Point Certified Security Expert (CCSE) - The advanced CCSE part of the course teaches how to build, modify, deploy and troubleshoot the R81.10 Check Point Security Systems on the GAiA operating system. Hands-on lab exercises teach how to debug firewall processes, optimize VPN performance and upgrade Management Servers. Goals: Validate and enhance your skills and optimally manage Check Point advanced security management systems. Topics: Management Upgrade and Migration, Management High Availability, Security Gateway Upgrades, Advanced Check Point Maintenance, Security Gateway

## Pre koho je kurz určený a požadované vstupné znalosti

Technical professionals who support, install deploy or administer Check Point products, and who perform advanced deployment configurations of Check Point products.

The Boot Camp courses helps delegates prepare for the CCSA and CCSE certification exams.

## Študijné materiály

Check Point guide book for this course.

## Osnova kurzu

### Check Point Certified Security Administrator (CCSA)

- Configure the Security Management Server.
- Use the WebUI to run the First Time Wizard.
- Install the Smart Console.
- Install the Alpha Gateway using the network detailed in the course topology.
- Demonstrate how the Security Management Server and Gateway communicate.
- Test SIC Status.
- Create multiple administrators and apply different roles and permissions for simultaneous administration.
- Validate existing licenses for products installed on the network.
- Create and configure host, network and group objects.
- Create a simplified Security Policy.
- Demonstrate how to use Security Zones in policy.
- Demonstrate how to share a layer between Security Policies.
- Configure Network Address Translation for server and network objects.
- Enable Identity Awareness.
- Deploy user access roles for more granular control of the security Policy.
- Generate network Traffic and use traffic visibility tools to monitor the data.
- Use SmartConsole and SmartView Monitor to view status, alerts, and block suspicious traffic.

### Check Point Certified Security Expert (CCSE)

- Prepare for a Security Management Server Upgrade
- Upgrade the Security Management Server
- Deploy a Secondary Security Management Server
- Configure a Distributed Log Server

#### GOPAS Praha

Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

#### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

#### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved

# Cybersecurity Boot Camp R81.10 (CCSA-CCSE)

- Upgrade a Security Gateway from SmartConsole
- Work with the Command Line
- Use Scripts and SmartTasks
- Configure Dynamic Objects
- Monitor Traffic
- Verify Policy Installation and Status
- Work with Gaia and Management APIs
- Work with Acceleration Features
- Configure a Locally Managed Site to Site VPN
- Configure a Site to Site VPN with an Interoperable Device
- Configure Remote Access VPN
- Configure Mobile Access VPN
- Configure a High Availability Cluster
- Work with ClusterXL
- Configure Policy Compliance
- Deploy SmartEvent

**GOPAS Praha**

Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Brno**

Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Bratislava**

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved