Check Point Certified Security Administrator (CCSA) R82

Kód kurzu: CCSAR

Tento kurz poskytuje študentom základné znalosti, zručnosti a praktické skúsenosti potrebné na konfiguráciu, správu a monitorovanie existujúceho prostredia Quantum Security.

Pre koho je kurz určený

- Security Administrators
- Security Engineers
- Security Analysts
- Security Consultants
- Security Architects

Čo Vás naučíme

Študenti sa naučia, ako pristupovať k portálu Gaia a k rozhraniu príkazového riadku Gaia, spravovať prístup administrátorov, vytvárať a konfigurovať sieťové objekty, vytvárať nové bezpečnostné politiky, konfigurovať vrstvy v definovanom poradí a zdieľanú vloženú vrstvu, analyzovať sieťovú prevádzku a monitorovať stav systému, konfigurovať identifikačné povedomie (Identity Awareness), zvýšiť úroveň zabezpečenia pomocou inšpekcie HTTPS, konfigurovať riadenie aplikácií a filtrovanie URL a nastaviť autonómnu prevenciu hrozieb.

Požadované vstupné znalosti

Base Knowledge

- Unix-like and/or Windows OS
- Internet Fundamentals
- Networking Fundamentals
- Networking Security
- System Administration
- TCP/IP Networking

Check Point Courses

- Check Point Deployment Administrator (suggested)

Osnova kurzu

Module 1: Introduction to Quantum Security

- Identify the primary components of the Check Point Three-Tier Architecture and explain how they work together in the Check Point environment.

Lab Tasks

- Explore Gaia on the Security Management Server
- Explore Gaia on the Dedicated Log Server
- Explore Gaia on the Security Gateway Cluster Members
- Connect to SmartConsole
- Navigate GATEWAYS &SERVERS Views
- Navigate SECURITY POLICIES Views
- Navigate LOGS &EVENTS Views
- Navigate MANAGE &SETTINGS Views

Module 2: Administrator Account Management

- Explain the purpose of SmartConsole administrator accounts.
- Identify useful features for administrator collaboration, such as session management, concurrent administration, and concurrent policy installation.

Lab Tasks

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

- Create New Administrators and Assign Profiles
- Test Administrator Profile Assignments
- Manage Concurrent Administrator Sessions
- Take Over Another Session and Verify Session Status

Module 3: Object Management

- Explain the purpose of SmartConsole Objects.
- Give examples of SmartConsole Physical and Logical Objects.

Lab Tasks

- View and Modify GATEWAYS &SERVERS Objects
- View and Modify Network Objects
- View and Modify Service Objects

Module 4: Security Policy Management

- Explain the purpose of Security Policies.
- Identify the essential elements of a Security Policy.
- Identify features and capabilities that enhance the configuration and management of the Security Policy.

Lab Tasks

- Verify the Security Policy
- Modify Security Policies
- Install the Standard Security Policy
- Test the Security Policy

Module 5: Policy Layers

- Demonstrate an understanding of the Check Point policy layer concept.
- Explain how policy layers affect traffic inspection.

Lab Tasks

- Add an Ordered Layer
- Configure and Deploy the Ordered Layer Rules
- Test the Ordered Layer Policy
- Create an Inline DMZ Layer
- Test the Inline DMZ Layer

Module 6: Security Operations Monitoring

- Explain the purpose of Security Operations Monitoring.
- Tune the Log Server configuration.
- Use predefined and custom queries to filter the logging results.
- Monitor the state of Check Point systems.

Lab Tasks

- Configure Log Management
- Enhance Rulebase View, Rules, and Logging
- Review Logs and Search for Data
- Configure the Monitoring Blade
- Monitor the Status of the Systems

Module 7: Identity Awareness

- Explain the purpose of the Identity Awareness solution.
- Identify the essential elements of Identity Awareness.

Lab Tasks

- Adjust the Security Policy for Identity Awareness
- Configure the Identity Collector
- Define the User Access Role

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

- Test Identity Awareness

Module 8: HTTPS Inspection

- Explain the purpose of the HTTPS Inspection solution.
- Identify the essential elements of HTTPS Inspection.

Lab Tasks

- Enable HTTPS Inspection
- Adjust Access Control Rules
- Deploy the Security Gateway Certificate
- Test and Analyze Policy with HTTPS Inspection

Module 9: Application Control and URL Filtering

- Explain the purpose of the Application Control and URL Filtering solutions.
- Identify the essential elements of Application Control and URL Filtering.

Lab Tasks

- Adjust the Access Control Policy
- Create and Adjust Application Control and URL
- Test and Adjust the Application Control and URL Filtering Rules

Module 10: Threat Prevention Fundamentals

- Explain the purpose of the Threat Prevention solution.
- Identify the essential elements of Autonomous Threat Prevention.

Lab Tasks

- Enable Autonomous Threat Prevention
- Test Autonomous Threat Prevention

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved