Check Point Certified Security Expert (CCSE) R82

Kód kurzu: CCSER

Tento kurz poskytuje účastníkom pokročilé znalosti, zručnosti a praktické skúsenosti potrebné na nasadenie, správu a monitorovanie existujúcich prostredí Quantum Security.

Pobočka	Dní	Katalógová cena	ITB
Praha	3	36 500 Kč	0
Bratislava	3	1 587 €	0

Všetky ceny sú uvedené bez DPH.

Termíny kurzu

Dátum	Dní	Cena kurzu	Typ výučby	Jazyk výučby	Lokalita
15.12.2025	3	36 500 Kč	Online	CZ/SK	Arrow ECS - Online
15.12.2025	3	36 500 Kč	Prezenčný	CZ/SK	Arrow ECS
15.12.2025	3	1 587 €	Online	CZ/SK	Online

Všetky ceny sú uvedené bez DPH.

Pre koho je kurz určený

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

Čo Vás naučíme

Účastníci sa naučia nasadiť vysokú dostupnosť správy (Management High Availability), pokročilú správu bezpečnostných politík, konfiguráciu Site-to-Site VPN, pokročilé monitorovanie bezpečnosti, aktualizáciu Security Gateway, použitie nástroja Central Deployment na inštaláciu hotfixov, import primárneho Security Management Servera, nasadenie klastra ElasticXL.

Požadované vstupné znalosti

Base Knowledge

- Unix-like and/or Windows OS
- Internet Fundamentals
- Networking Fundamentals
- Networking Security
- System Administration
- TCP/IP Networking
- Text Editors in Unix-like OS
- Minimum of 6-months of practical experience with the management of a Quantum Security Environment.

Check Point Courses

- Check Point Certified Security Administrator (required)
- Check Point Deployment Administrator (suggested)

Študijné materiály

Príručka ku kurzu firmy Check Point podľa programu kurzu.

Osnova kurzu

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Module 1: Management High Availability
- Explain the purpose of Management High Availability.
- Identify the essential elements of Management High Availability.

Lab Tasks
- Deploy and configure Management High Availability
- Ensure the failover process functions as expected

Module 2: Advanced Policy Management
- Identify ways to enhance the Security Policy with more object types.
- Create dynamic objects to make policy updatable from the Gateway.
- Manually define NAT rules.
- Configure Security Management behind NAT.

Lab Tasks
- Use Updatable Objects
- Configure Network Address Translation for server and network objects
- Configure Management behind NAT for Branch Office connections

Module 3: Site-to-Site VPN
- Discuss site-to-site VPN basics, deployment, and communities.
- Describe how to analyze and interpret VPN tunnel traffic.
- Articulate how pre-shared keys and certificates can be configured to authenticate with third-party and externally managed VPN Gateways.
- Explain Link Selection and ISP Redundancy options.
- Explain tunnel management features.

Lab Task
- Configure Site-to-Site VPN with internally managed Security Gateways

Module 4: Advanced Security Monitoring
- Describe the SmartEvent and Compliance Blade solutions, including their purpose and use.

Lab Tasks
- Configure a SmartEvent Server to monitor relevant patterns and events
- Demonstrate how to configure Events and Alerts in SmartEvent
- Demonstrate how to run specific SmartEvent reports
- Activate the Compliance Blade
- Demonstrate Security Best Practice settings and alerts
- Demonstrate Regulatory Requirements Compliance Scores

Module 5: Upgrades
- Identify supported upgrade options.

Lab Task
- Upgrade a Security Gateway
- Use Central Deployment tool to install Hotfixes

Module 6: Advanced Upgrades and Migrations
- Export/import a Management Database.
- Upgrade a Security Management Server by freshly deploying the new release or using a new appliance.

Lab Task
- Prepare to perform an Advanced Upgrade with Database Migration on the Primary Security Management Server in a distributed environment
- Perform an import of a Primary Security Management Server in a distributed Check Point environment

Module 7: ElasticXL Cluster

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Describe the ElasticXL Cluster solution, including its purpose and use.

Lab Tasks

- Deploy an ElasticXL Security Gateway Cluster

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk