IBM QRadar SIEM Foundations

Kód kurzu: BQ105G

IBM Security QRadar enables deep visibility into network, endpoint, user, and application activity. It provides collection, normalization, correlation, and secure storage of events, flows, assets, and vulnerabilities. Suspected attacks and policy breaches are highlighted as offenses. In this course, you learn about the solution architecture, how to navigate the user interface, and how to investigate offenses. You search and analyze the information from which QRadar concluded a suspicious activity. Hands-on exercises reinforce the skills learned.

Pobočka	Dní	Katalógová cena	ITB
Praha	3	42 000 Kč	0
Brno	3	42 000 Kč	0
Bratislava	3	1 640 €	0

Všetky ceny sú uvedené bez DPH.

Termíny kurzu

Dátum	Dní	Cena kurzu	Typ výučby	Jazyk výučby	Lokalita
25.05.2026	3	42 000 Kč	Online	CZ/SK	TD SYNNEX Czech - Online
25.05.2026	3	42 000 Kč	Prezenčný	CZ/SK	TD SYNNEX Czech
25.05.2026	3	1 640 €	Online	CZ/SK	Online
15.06.2026	3	42 000 Kč	Prezenčný	CZ/SK	TD SYNNEX Czech
15.06.2026	3	42 000 Kč	Online	CZ/SK	TD SYNNEX Czech - Online
15.06.2026	3	1 640 €	Online	CZ/SK	Online
20.07.2026	3	42 000 Kč	Online	EN	TD SYNNEX Czech - Online
14.09.2026	3	1 640 €	Online	CZ/SK	Online
14.09.2026	3	42 000 Kč	Online	CZ/SK	TD SYNNEX Czech - Online
14.09.2026	3	42 000 Kč	Prezenčný	CZ/SK	TD SYNNEX Czech
26.10.2026	3	42 000 Kč	Online	EN	TD SYNNEX Czech - Online
30.11.2026	3	42 000 Kč	Online	CZ/SK	TD SYNNEX Czech - Online
30.11.2026	3	42 000 Kč	Prezenčný	CZ/SK	TD SYNNEX Czech
30.11.2026	3	1 640 €	Online	CZ/SK	Online

Všetky ceny sú uvedené bez DPH.

Pre koho je kurz určený

This course is designed for security analysts, security technical architects, offense managers, network administrators, and system administrators using QRadar SIEM.

Čo Vás naučíme

In this 3-day instructor-led course, you learn how to perform the following tasks:

- Describe how QRadar collects data to detect suspicious activities
- Describe the QRadar architecture and data flows
- Navigate the user interface
- Define log sources, protocols, and event details
- Discover how QRadar collects and analyzes network flow information
- Describe the QRadar Custom Rule Engine

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

- Utilize the Use Case Manager app
- Discover and manage asset information
- Learn about a variety of QRadar apps, content extensions, and the App Framework
- Analyze offenses by using the QRadar UI and the Analyst Workflow app
- Search, filter, group, and analyze security data
- Use AQL for advanced searches
- Use QRadar to create customized reports
- Explore aggregated data management
- Define sophisticated reporting using Pulse Dashboards
- Discover QRadar administrative tasks

Extensive lab exercises are provided to allow learners an insight into the routine work of an IT Security Analyst operating the QRadar SIEM platform. The exercises cover the following topics:

- Architecture exercises
- UI Overview exercises
- Log Sources exercises
- Flows and QRadar Network Insights exercises
- Custom Rule Engine (CRE) exercises
- Use Case Manager app exercises
- Assets exercises
- App Framework exercises
- Working with Offenses exercises.
- Search, filtering, and AQL exercises
- Reporting and Dashboards exercises
- QRadar Admin tasks exercises

The lab environment for this course uses the IBM QRadar SIEM 7.5 platform.

After completing this course, you should be able to perform the following tasks:

- Describe how QRadar collects data to detect suspicious activities
- Describe the QRadar architecture and data flows
- Navigate the user interface
- Define log sources, protocols, and event details
- Discover how QRadar collects and analyzes network flow information
- Describe the QRadar Custom Rule Engine
- Utilize the Use Case Manager app
- Discover and manage asset information
- Learn about a variety of QRadar apps, content extensions, and the App Framework
- Analyze offenses by using the QRadar UI and the Analyst Workflow app
- Search, filter, group, and analyze security data
- Use AQL for advanced searches
- Use QRadar to create customized reports
- Explore aggregated data management
- Define sophisticated reporting using Pulse Dashboards
- Discover QRadar administrative tasks

Požadované vstupné znalosti

Before taking this course, make sure that you have the following skills:

- IT infrastructure
- IT security fundamentals
- Linux

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

- Windows
- TCP/IP networking
- Syslog

Študijné materiály

Studijní materiál IBM

Osnova kurzu

- Unit 0: IBM Security QRadar 7.5 – Fundamentals
- Unit 1: QRadar Architecture
- Unit 2: QRadar UI – Overview
- Unit 3: QRadar – Log Source
- Unit 4: QRadar flows and QRadar Network Insights
- Unit 5: QRadar Custom Rule Engine (CRE)
- Unit 6: QRadar Use Case Manager app
- Unit 7: QRadar – Assets
- Unit 8: QRadar extensions
- Unit 9: Working with Offenses
- Unit 10: QRadar – Search, filtering, and AQL
- Unit 11: QRadar – Reporting and Dashboards
- Unit 12: QRadar – Admin Console

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