

IBM QRadar SIEM Advanced Topics

Kód kurzu: BQ205G

QRadar SIEM provides deep visibility into network, 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. This 2-day instructor-led course walks you through various advanced topics about QRadar such as custom log sources, reference data collections and custom rules, X-Force data and the Threat Intelligence app, UBA and QRadar Advisor, tuning and custom action scripts. The course also discusses integration with IBM SOAR. Hands-on exercises reinforce the skills learned. The lab environment for this course uses the IBM QRadar SIEM 7.5 platform.

Pobočka	Dnů	Cena kurzu	ITB
Praha	2	26 800 Kč	0
Bratislava	2	1 075 €	0

Uvedené ceny jsou bez DPH.

Termíny kurzu

Datum	Dnů	Cena kurzu	Typ výuky	Jazyk výuky	Lokalita
G 28.11.2024	2	26 800 Kč	Online	CZ/SK	Partner online live
G 28.11.2024	2	26 800 Kč	Prezenční	CZ/SK	Praha - TD Synnex Academy
27.02.2025	2	26 800 Kč	Prezenční	CZ/SK	Praha - TD Synnex Academy
27.02.2025	2	26 800 Kč	Online	CZ/SK	Partner online live
29.05.2025	2	26 800 Kč	Prezenční	CZ/SK	Praha - TD Synnex Academy
29.05.2025	2	26 800 Kč	Online	CZ/SK	Partner online live
18.09.2025	2	26 800 Kč	Prezenční	CZ/SK	Praha - TD Synnex Academy
18.09.2025	2	26 800 Kč	Online	CZ/SK	Partner online live
04.12.2025	2	26 800 Kč	Online	CZ/SK	Partner online live
04.12.2025	2	26 800 Kč	Prezenční	CZ/SK	Praha - TD Synnex Academy

Uvedené ceny jsou bez DPH.

Pro koho je kurz určen

This course is designed for security administrators and security analysts.

Co Vás naučíme

- Learn how to create custom log sources
- Discover how to work with reference data collections and custom rules
- Use X-Force data and Threat Intelligence app
- Use the Use Case Manager app
- Learn how to use UBA and QRadar Advisor
- Discover Tuning
- Explore Custom action scripts
- Discuss Integration with IBM SOAR

Požadované vstupní znalosti

Students should be knowledgeable about the following topics:

- 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



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

IBM QRadar SIEM Advanced Topics

- Windows
- TCP/IP networking
- Syslog
- Foundational skills for the IBM QRadar Security Intelligence Platform (at least the skills that are taught in the IBM QRadar SIEM Foundations - BQ104 course)

Studijní materiály

Studijní materiál IBM

Osnova kurzu

- Custom log sources
- Reference data collections and custom rules
- IBM X-Force Threat Intelligence in QRadar
- User Behavior Analytics and Advisor with Watson
- Tuning
- Custom action scripts
- IBM SOAR integration

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



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