



**Enterprise Computing Solutions - Education Services**

## **TRAINING OFFERING**

---

**Skontaktuj się z nami**

Email: [szkolenia.ecs.pl@arrow.com](mailto:szkolenia.ecs.pl@arrow.com)  
Phone: 12 616 43 00



## IBM QRadar SIEM Advanced Topics

**Kod:**            **Czas trwania:**            **Cena netto:**

BQ204G        16 Hours (2 days)            zł4,300.00

### Description

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 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 7.4 platform.

### Cel szkolenia

- 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

### Uczestnicy

This course is designed for security administrators and security analysts.

### Wymagania wstępne

Students should be knowledgeable about the following topics:

- IT infrastructure
- IT security fundamentals
- Linux
- 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)

### Program szkolenia

Unit 1: Custom log sources    Unit 2: Reference data collections and custom rules    Unit 3: IBM X-Force Threat Intelligence in QRadar  
Unit 4: User Behavior Analytics and Advisor with Watson    Unit 5: Tuning    Unit 6: Custom action scripts    Unit 7: IBM SOAR integration

### Terminy

Data	Lokalizacja	Strefa czasowa	Język	Typ szkolenia	Gwarancja	Cena netto
27 May 2024	Virtual Classroom	CEDT	Polish	Instructor Led Online		zł4,300.00

## Dodatkowe informacje

Jeśli interesują Cię inne szkolenia tego producenta - skontaktuj się z nami.