



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Skontaktuj się z nami

Email: szkolenia.ecs.pl@arrow.com
Phone: 12 616 43 00



IBM QRadar SIEM Foundations

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

BQ105XG 24 Hours zł6,650.00

Description

This course is designed and built on QRadar 7.4.3 and QRadar 7.5.0. The lab is based on QRadar 7.5.0 update 8. **What you learn:**

- 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

Skills you gain:

- Threat investigation
- QRadar data searching

Cel szkolenia

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

Uczestnicy








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

Wymagania wstępne

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

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Syslog

Program szkolenia

- Unit 0: IBM Security QRadar 7.4  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

Terminy

| Data | Lokalizacja | Strefa czasowa | Język | Typ szkolenia | Gwarancja | Cena netto |
|-------------|-------------|----------------|---------|---------------------|-----------|------------|
| 23 Nov 2024 | | | English | Self Paced Training | | zł6,650.00 |

Dodatkowe informacje

[Jeśli interesują Cię inne szkolenia tego producenta - skontaktuj się z nami.](#)