



## TRAINING OFFERING

---

**You can reach us at:**

Arrow ECS, Nidderdale House, Beckwith Knowle, Harrogate, HG3 1SA

Email: [educationteam.ecs.uk@arrow.com](mailto:educationteam.ecs.uk@arrow.com)

Phone: 0870 251 1000



## IBM QRadar SIEM Advanced Topics

<b>CODE:</b>	<b>LENGTH:</b>	<b>PRICE:</b>
BQ205G	16 Hours (2 days)	£1,300.00

### 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 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.

### Objectives

- 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

### Audience

This course is designed for security administrators and security analysts.

### Prerequisites

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)

### Programme

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

### Session Dates

On request. Please [Contact Us](#)

## **Additional Information**

This training is also available as onsite training. Please contact us to find out more.