
IBM QRadar SIEM Advanced Topics

Duration: 2 Days **Course Code: BQ205G** **Delivery Method: Virtual Learning**

Overview:

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.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

This course is designed for security administrators and security analysts.

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
-

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)
-

Content:

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

Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A, First Floor, Office F68, Dubai, UAE