IBM Security QRadar SIEM Advanced Topics

Duration: 2 Days   Course Code: BQ203G

Overview:

This is an advanced course for the QRadar Analyst and Administrator and is a follow-on to BQ103G.
This course uses the IBM QRadar SIEM 7.3 platform for lab exercises.

Target Audience:

This course is useful for Security administrators, Security technical architects, Offense managers, Professional services using QRadar SIEM, QRadar SIEM administrators.

Objectives:

- The course objctives are:
- Create custom log sources to utilize events from uncommon sources
- Create, maintain, and use reference data collections
- Develop and manage custom rules to detect unusual activity in your network
- Develop and manage custom action scripts to for automated rule reponse
- Develop and manage anomoly detection rules to detect when unusual network traffic patterns occur

Prerequisites:

Before this course, you should be familiar with:

- IT infrastructure
- IT security fundamentals
- Linux
- Microsoft Windows
- TCP/IP networking
- Log files and events
- Network flows

You should also have completed the IBM QRadar SIEM Foundations course.

Content:

In this course, you will see:

- Module 1: Creating log source types
- Module 2: Leveraging reference data collections
- Module 3: Developing custom rules
- Module 4: Creating Custom Action Scripts
- Module 5: Developing Anomaly Detection Rules

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/