IBM QRadar SIEM Advanced Topics (BQ203G)

Course ID #: 0370-203-BQ203G-W

Hours: 14

Course Content

Course Description:

This is an advanced course for the QRadar Analyst and Administrator and is a follow-on to BQ103G.

Course Objectives:

After completing this course, you should be able to:

- 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

Target Audience:

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

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.

Topics:

- **Creating log source types**
- **Leveraging reference data collections**
- **Developing custom rules**
- **Creating Custom Action Scripts**
- **Developing Anomaly Detection Rules**