IBM SECURITY QRADAR SIEM ADVANCED TOPICS

DUARTION: 2 DAYS

COURSE 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.

COURSE OBJECTIVES

The course objectives are:

1. Create custom log sources to utilize events from uncommon sources
2. Create, maintain, and use reference data collections
3. Develop and manage custom rules to detect unusual activity in your network
4. Develop and manage custom action scripts to for automated rule response
5. Develop and manage anomoly detection rules to detect when unusual network traffic patterns occur

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

COURSE PREREQUISITES

Before this course, you should be familiar with:

1. IT infrastructure
2. IT security fundamentals
3. Linux
4. Microsoft Windows
5. TCP/IP networking
6. Log files and events
7. Network flows

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