

Course Code: BQ204G

Course Title: IBM QRadar SIEM Advanced Topics

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 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 7.4 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

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)

Duration:

16 Hrs

Topics:

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

Audience:

This course is designed for security administrators and security analysts.