

IBM QRadar SIEM Advanced Topics (2 Days)

IBM® Security QRadar® enables you to minimize the time gap between when a suspicious activity occurs and when you detect it. Attacks and policy violations leave their footprints in log events and network flows of your IT systems. To connect the dots, QRadar SIEM correlates these scattered events and flows into offenses that alert you to suspicious activities. Using the skills taught in this course, you will be able to configure processing of uncommon events, work with reference data, and develop custom rules, custom actions, and custom anomaly detection rules.

Skills Gained

- 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 anomaly detection rules to detect when unusual network traffic patterns occur

Who Can Benefit

- Security administrators
- Security technical architects
- Offense managers
- Professional services using QRadar SIEM
- QRadar SIEM administrators

Prerequisites

- 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.

Course Outline

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