IBM QRadar SIEM Advanced Topics

Trainings-ID: BQ203

Zum Seminar →

Das nehmen Sie mit

- 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

Zielgruppen

Audience

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

Wichtige Informationen

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 anomoly detection rules.

The lab environment for this course uses the IBM QRadar SIEM 7.3 platform.

Termine & Optionen