

IBM QRadar SIEM Advanced Topics (BQ203G)

ID BQ203G **Preis** CHF 1'700.– (exkl. MwSt.) **Dauer** 2 Tage

Zielgruppe

Audience

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

Voraussetzungen

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.

Kursinhalt

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.

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

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer GmbH

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>