IBM Security QRadar SIEM Advanced Topics

Information

Length:	1.0 Day
__Ref:	BQ132G-X
Delivery method:	ClassroomInstructor Led Online
Price:	EUR

Overview

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.

Public

Audience

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

Prerequisits

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 Security QRadar SIEM Foundations course.

Objective

- Create custom log sources to utilize events from uncommon sources
- Create, maintain, and use reference data collections
- Develop and optimize custom rules to detect indicators of an attack or policy violation

Topics

Module 1: Creating custom log sources
Module 2: Leveraging reference data collections
Module 3: Developing custom rules