IBM QRadar SIEM Foundations (BQ103G)

Zielgruppe

This course is designed for security analysts, security technical architects, offense managers, network administrators, and system administrators using QRadar SIEM.

Voraussetzungen

Before taking this course, make sure that you have the following skills:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Syslog

Kursinhalt

IBM QRadar SIEM provides deep visibility into network, user, and application activity. It provides collection, normalization, correlation, and secure storage of events, flows, asset profiles, and vulnerabilities. QRadar SIEM classifies suspected attacks and policy violations as offenses.

In this 3-day instructor-led course, you learn how to perform the following tasks:

- Describe how QRadar SIEM collects data to detect suspicious activities
- Describe the QRadar SIEM component architecture and data flows
- Navigate the user interface
- Investigate suspected attacks and policy breaches
- Search, filter, group, and analyze security data
- Investigate the vulnerabilities and services of assets
- Use network hierarchies
- Locate custom rules and inspect actions and responses of rules
- Analyze offenses created by QRadar SIEM
- Use index management

- Navigate and customize the QRadar SIEM dashboard
- Use QRadar SIEM to create customized reports
- Use charts and filters
- Use AQL for advanced searches
- Analyze a real world scenario

Extensive lab exercises are provided to allow students an insight into the routine work of an IT Security Analyst operating the IBM QRadar SIEM platform. The exercises cover the following topics:

- Using the QRadar SIEM user interface
- Investigating an Offense triggered by events
- Investigating the events of an offense
- Investigating an offense that is triggered by flows
- Using rules
- Using the Network Hierarchy
- Index and Aggregated Data Management
- Using the QRadar SIEM dashboard
- Creating QRadar SIEM reports
- Using AQL for advanced searches
- Analyze a real-world large-scale attack

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