

IBM QRadar SIEM Foundations

Learn to investigate offenses, analyse events and flows, and build reports and searches using IBM QRadar SIEM.

COURSE OVERVIEW

This course covers the architecture and data flows of IBM QRadar SIEM and navigation of its user interface. It addresses investigating offenses triggered by events and by flows, using asset profiles, rules, and the network hierarchy to support that analysis. It also covers index and aggregated data management, the dashboard, report creation, filters, and the Ariel Query Language for advanced searches, concluding with analysis of a real-world large-scale attack.

WHO THIS COURSE IS FOR

SOC Analysts

Security Analysts

Incident Responders

SIEM Administrators

Network Security Engineers

15 Modules

01

Introduction to IBM QRadar

02

IBM QRadar SIEM Component Architecture and Data Flows

03

Using the QRadar SIEM User Interface

04

Investigating an Offense Triggered by Events

05

Investigating the Events of an Offense

06

Using Asset Profiles to Investigate Offenses

07

Investigating an Offense Triggered by Flows

08

Using Rules

09

Using the Network Hierarchy

10

Index and Aggregated Data Management

11

Using the QRadar SIEM Dashboard

12

Creating Reports

13

Using Filters

14

Using the Ariel Query Language (AQL) for Advanced Searches

15

Analyzing a Real-World Large-Scale Attack

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com