

# IBM Certified Associate Administrator - IBM QRadar SIEM

Learn to implement, configure, monitor and troubleshoot IBM QRadar SIEM deployments, from installation to upgrades and performance checks.

**5**

MODULES

**31**

TOPICS

## COURSE OVERVIEW

This course covers planning and implementing a QRadar deployment, including installation and adding managed hosts, followed by migration and upgrade tasks such as reviewing release notes, applying patches, and backing up or restoring content. It then addresses configuration and administration activities, covering event flow sources, user roles and security profiles, license management, rules and reference sets, retention policies, searches, dashboards, reports, network hierarchy, domains and tenants, the asset database, and vulnerability scans. The course also covers monitoring QRadar through notifications, system dashboards, processes, performance, and dedicated apps, as well as checking appliance health and detecting offenses and anomalies. Finally, it covers troubleshooting QRadar using key commands, error messages, log interpretation, and embedded troubleshooting tools.

## WHO THIS COURSE IS FOR

SIEM Administrators

Security Analysts

System Administrators

Security Operations Staff

Network Security Engineers

## LEARNING OBJECTIVES

- Plan and implement a QRadar deployment with managed hosts
- Perform QRadar upgrades, patches and migrations
- Configure event flow sources and custom properties
- Administer users, user roles and security profiles
- Manage rules, building blocks and reference sets
- Configure retention policies, dashboards and reports
- Monitor QRadar performance, processes and notifications
- Interpret logs and apply troubleshooting tools

## 5 Modules, 31 Topics

01

### Implementing

#### TOPICS

Plan and design QRadar deployment · Implement and install QRadar · Add Managed Hosts

02

### Migrating and Upgrading

#### TOPICS

- Plan QRadar upgrade and migration
- Review documentation and release notes
- Perform QRadar updates, patches and upgrades
- Perform migration (e.g., backup and restore, import and export content)

03

### Configuring and Administering Tasks

#### TOPICS

- Configure event flow sources and custom properties
- Maintain configuration and data backups
- Create and administer users, user roles, and security profiles
- Manage the license per allocation
- Create, review and modify rules, building blocks and reference sets
- Configure and manage retention policies (i.e., data and assets)
- Create and manage saved searches, index, global views, dashboards and reports
- Deploy and manage applications and content packages
- Configure global system notifications
- Configure and apply network hierarchy
- Configure and manage domain and tenants
- Use the asset database
- Schedule and run a VA scan

## 04

### Monitoring

#### TOPICS

- Monitor QRadar Notifications and error messages
- Review and interpret system monitoring dashboards
- Verify QRadar processes and services
- Monitor QRadar performance
- Use apps and tools for monitoring (e.g., QDI, assistant app, incident overview, DrQ)
- Check system maintenance and health of appliances
- Monitor offenses and detect anomalies

## 05

### Troubleshooting

#### TOPICS

- Demonstrate knowledge of key commands to interpret QRadar services and processes
- Explain error messages and notifications
- Interpret the basic logs (e.g., qradar.error, qradar.log)
- Use embedded troubleshooting tools and scripts

#### 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](https://koenig-solutions.com)

✉ [info@koenig-solutions.com](mailto:info@koenig-solutions.com)