Updated on 10/01/2025

Sign up

IBM QRadar SOAR training

3 days (21 hours)

Presentation

Our IBM QRadar SOAR training will teach you the skills you need to automate your security through workflow integration. Our program covers all the tool's functionalities, so you can effectively analyze and deal with cyber attacks.

In this course, you'll begin by gaining an in-depth understanding of SOAR and IBM QRadar SOAR's place in your IT environment. Through a hands-on demonstration, you'll learn how to manipulate the interface and configure your alerts.

You'll learn about best practices, role management, incident management and workflow. Threat response automation and orchestration with IBM QRadar SOAR.

As with all our training courses, we will introduce you to the latest version of the software: IBM QRadar SOAR V51.0.0

Objectives

- Understand the importance of a SOAR in cybersecurity and its various functions
- Installing and configuring QRadar
- Mastering third-party systems integration
- Using QRadar's advanced features
- JSON-structured data integration

Target audience

- **Cybersecurity Analysts**
- SOC Analysts
- SOC Managers

- Safety engineer
- DevSecOps
- Network Administrator

Prerequisites

Basic knowledge of networks and systems.

Hardware requirements

Access to IBM QRadar SOAR.

IBM QRadar SOAR training program

INTRODUCTION TO SOAR

- Understanding the importance of a SOAR
- SOAR's role in cybersecurity
- SIEM vs SOAR
- SOAR guidelines and architecture
- Initial configuration of QRadar SOAR
- Connection with QRadar SIEM and other tools

PRESENTATION OF QRADAR

- The components
- Data flows
- Getting to grips with the interface
- Fundamental concepts of QRadar
- The tool's main functions

MANAGEMENT AND ADMINISTRATION

- Install QRadar
- Configuration
- Migration procedures
- Upgrade
- Understanding the incident lifecycle
- Strategies for managing backups and restoring data
- Security and user access management
- Case management and response prioritization
- Troubleshooting

Automation and Orchestration

- Introduction to playbook concepts
- Studying the JSON structure of playbooks
- Create automated workflows
- Workflows against phishing
- Workflows against ransomware
- Automation of SOC tasks
- Integration with threat analysis tools

MONITORING WITH QRADAR

- Monitoring and interpreting QRadar notifications
- How to use dashboards
- Investigate detected anomalies
- Notification configuration
- Good monitoring practices
- Strategies for monitoring asset changes
- Detecting associated risks
- Recommended practices for asset information maintenance

Perfecting QRadar SOAR

- Third-party systems integration
  - Antivirus
  - Firewall
  - Cloud platforms
- Using APIs to customize workflows
- Analysis of SOC metrics to identify bottlenecks
- Use QRadar APIs to integrate JSON-structured data

ADMINISTRATION CONSOLE

- Using the administration console
- Defense against multi-vector attacks
- Internal compromise
- Best practices for managing configurations and security parameters

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as enrolment is finalized, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and objectives.

This questionnaire also enables us to anticipate any connection or internal security problems (intra-company or virtual classroom) that could be problematic for the follow-up and smooth running of the training session. This questionnaire also enables us to anticipate any connection or internal security difficulties (intra-company or virtual classroom) that could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.