+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 05/28/2024

Sign up

IBM QRadar SIEM training

4 days (28 hours)

Presentation

Our IBM QRadar SIEM training course will teach you to master one of the most widely adopted SIEM software packages in the world. In fact, our program covers all the tool's functionalities, so that you can effectively analyze and deal with cybercriminal attacks.

In this course, you'll begin by gaining an in-depth understanding of SIEM and IBM QRadar SIEM'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, logs and data flows. Investigation and monitoring with IBM QRadar SIEM will hold no secrets for you.

As with all our training courses, we'll be presenting the latest version of the software: IBM QRadar 7.4.3.

Objectives

- Understand the importance of a SIEM in cybersecurity and its various functions
- Installing and configuring QRadar
- Integrating and managing logs
- Using QRadar's advanced features

Target audience

- **Cybersecurity Analysts**
- SOC Analysts
- Cybersecurity Officer
- System Administrator
- Network Administrator

Prerequisites

Basic knowledge of networks and systems.

Hardware requirements

Access to IBM QRadar SIEM.

IBM QRadar SIEM training program

INTRODUCTION TO SIEM

- Understanding the importance of a SIEM
- The role of SIEM in cybersecurity
- SIM vs SEM
- SIEM guidelines and architecture
- Overview of key SIEM capabilities:
  - Aggregation
  - Correlation
  - Reporting
  - Storage
  - Alerts
  - Automation

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
- Tuning techniques to optimize performance
- Strategies for managing backups and restoring data
- Security and user access management
- Troubleshooting

LOGS AND FEEDS

- Log integration
- Log standardization
- Event management
- Methods for analyzing attack-related events
- Log source configuration
- Preparing for data analysis
- Search tools
- Filtering 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

INVESTIGATION

- Vulnerability investigation techniques
- Using index management and aggregated data for efficient searches
- Introduction to Ariel Query Language (AQL) for advanced searches
- Analysis of real-life cases
- Creation of investigation reports

ADMINISTRATION CONSOLE

- Using the administration console
- Attack simulation
- Process analysis with Sysmon
- Best practices for managing configurations and security parameters

ADVANCED OPERATIONS

- QRadar integration with other systems
- Manage custom log source types
- Using and configuring reference data collections
- Creating custom rules
- Using QRadar extensions
- Extension management
- Best practices for customizing QRadar

Companies concerned

This training 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 registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which 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, with 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.