Publication date : 02/05/2024

Course : IBM QRadar SIEM, the basics

Practical course - 3d - 21h - Ref. IBF
Price : 2470 CHF E.T.

QRadar is an event correlation tool for collecting and sorting relevant information generated by various security devices. This course will enable you to configure the application, analyze the data flow and generate reports based on pre-configured alerts.

Teaching objectives

At the end of the training, the participant will be able to:

- Collect, analyze and report on data with QRadar
- Enrich operational data with searches and feeds
- Create real-time alerts
- Generate reports

Intended audience

System and network administrators.

Prerequisites

Basic knowledge of networks and systems.

Course schedule

1 SIEM

- What is a SIEM (Security Information Event Management)?
- Why correlate events?
- SIEM tools on the market.

PARTICIPANTS

System and network administrators.

PREREQUISITES

Basic knowledge of networks and systems.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

2 QRadar architecture and interface

- Introduction and positioning of the QRadar tool.
- How to configure QRadar SIEM to collect data.
- Learn to detect suspicious activity.
- QRadar SIEM architecture and data flow components.
- The QRadar user interface.

Hands-on work
Getting to grips with the QRadar interface.

3 Analysis and search for suspicious actions

- Investigate suspicious attacks.
- Search for security policy violations.
- Search, filter, group and analyze safety data.
- Analyze events and flows.
- Investigate asset profiles.

Hands-on work
Search for attacks or security policy violations. Create real-time alerts.

4 Rules and index management

- Why the network hierarchy.
- Determine how rules examine incoming data and create violations.
- How to use indexes and aggregate data management.

Hands-on work
Examine incoming data and create violations. Use rules and indexes.

5 Dashboards

- Dashboard management.
- The different elements of a dashboard.
- How do I move between dashboards?
- Customize dashboards and their elements.

Hands-on work
Customize dashboards.

6 Reports

- Presentation of reports.
- General parameters.
- Report objects and their parameters.
- Create customized reports.

Hands-on work
Create and use reports.

7 Filters and advanced search

- Quickly available and usable filters.
- Use filters to perform a search.
- Use of AQL (Ariel Query Language) for advanced searches.

Hands-on work
Set up filters and use advanced searches.

TERMS AND DEADLINES
Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES
Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

Dates and locations

REMOTE CLASS
2026 : 16 Mar., 22 June, 7 Oct., 16 Nov.