



Enterprise Computing Solutions - Education Services

## TRAINING OFFERING

---

**Du kan nå oss här**

Kronborgsgränd 7, 164 46 Kista

Email: [edu.ecs.se@arrow.com](mailto:edu.ecs.se@arrow.com)

Phone: +46 8 555 188 00



# IBM QRadar SIEM Foundations

| <b>CODE:</b> | <b>LENGTH:</b> | <b>PRICE:</b> |
|--------------|----------------|---------------|
| BQ105XG      | 24 Hours       | kr12,653.00   |

## Description

This course is designed and built on QRadar 7.4.3 and QRadar 7.5.0. The lab is based on QRadar 7.5.0 update 8. **What you learn:**

- Describe how QRadar collects data to detect suspicious activities
- Describe the QRadar architecture and data flows
- Navigate the user interface
- Define log sources, protocols, and event details
- Discover how QRadar collects and analyzes network flow information
- Describe the QRadar Custom Rule Engine
- Utilize the Use Case Manager app
- Discover and manage asset information
- Learn about a variety of QRadar apps, content extensions, and the App Framework
- Analyze offenses by using the QRadar UI and the Analyst Workflow app
- Search, filter, group, and analyze security data
- Use AQL for advanced searches
- Use QRadar to create customized reports
- Explore aggregated data management
- Define sophisticated reporting using Pulse Dashboards
- Discover QRadar administrative tasks

## Skills you gain:

- Threat investigation
- QRadar data searching

## Objectives

After completing this course, you should be able to perform the following tasks:

- Describe how QRadar collects data to detect suspicious activities
- Describe the QRadar architecture and data flows
- Navigate the user interface
- Define log sources, protocols, and event details
- Discover how QRadar collects and analyzes network flow information
- Describe the QRadar Custom Rule Engine
- Utilize the Use Case Manager app
- Discover and manage asset information
- Learn about a variety of QRadar apps, content extensions, and the App Framework
- Analyze offenses by using the QRadar UI and the Analyst Workflow app
- Search, filter, group, and analyze security data
- Use AQL for advanced searches
- Use QRadar to create customized reports
- Explore aggregated data management
- Define sophisticated reporting using Pulse Dashboards
- Discover QRadar administrative tasks

## Audience








This course is designed for security analysts, security technical architects, offense managers, network administrators, and system administrators using QRadar SIEM.

## Prerequisites

Before taking this course, make sure that you have the following skills:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Syslog

## Programme

- Unit 0: IBM Security QRadar 7.4  Fundamentals
- Unit 1: QRadar Architecture
- Unit 2: QRadar UI  Overview
- Unit 3: QRadar  Log Source
- Unit 4: QRadar flows and QRadar Network Insights
- Unit 5: QRadar Custom Rule Engine (CRE)
- Unit 6: QRadar Use Case Manager app
- Unit 7: QRadar  Assets
- Unit 8: QRadar extensions
- Unit 9: Working with Offenses
- Unit 10: QRadar  Search, filtering, and AQL
- Unit 11: QRadar  Reporting and Dashboards
- Unit 12: QRadar  Admin Console

## Session Dates

| Date        | Location | Time Zone | Language | Type                | Guaranteed | PRICE       |
|-------------|----------|-----------|----------|---------------------|------------|-------------|
| 22 Nov 2024 |          |           | English  | Self Paced Training |            | kr12,653.00 |

## Ytterligare information

[Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.](#)