TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

IBM QRadar SIEM Advanced Topics

CODE:	LENGTH:	PRICE:
BQ205XG	16 Hours	kr9,865.00

Description

This course is designed and built on IBM Security� QRadar� 7.4.3. and QRadar 7.5.0. The lab is built on QRadar 7.5.0 update 8.
What you learn:

- Create custom log sources
- Work with reference data collections and custom rules
- Use X-Force data and Threat Intelligence app
- Use the Use Case Manager app
- Use User Behavior Analytics (UBA) and QRadar Advisor
- Discover and perform tuning
- Explore custom action scripts
- Integrate QRadar with IBM SOAR

Skills you gain:

- Threat investigation
- QRadar data searching
- QRadar X-Force integration
- QRadar incident response

Objectives

- Learn how to create custom log sources
- Discover how to work with reference data collections and custom rules
- Use X-Force data and Threat Intelligence app
- Use the Use Case Manager app
- Learn how to use UBA and QRadar Advisor
- Discover Tuning
- Explore Custom action scripts
- Discuss Integration with IBM SOAR

Audience

This course is designed for security administrators and security analysts.

Prerequisites

Students should be knowledgeable about the following topics:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Syslog
- Foundational skills for the IBM QRadar Security Intelligence Platform (at least the skills that are taught in the IBM QRadar SIEM Foundations - BQ104 course)

Programme

Unit 1: Custom log sourcesUnit 2: Reference data collections and custom rulesUnit 3: IBM X-Force Threat Intelligence in QRadar Unit 4: User Behavior Analytics and Advisor with WatsonUnit 5: TuningUnit 6: Custom action scriptsUnit 7: IBM SOAR integration

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
01 Jan 0001			English	Self Paced Training		kr9,865.00

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.