IBM QRadar SIEM Advanced Topics (BQ204G)

ID BQ204G **Prix** CHF 1 600,– (Hors Taxe) **Durée** 2 jours

A qui s'adresse cette formation

This course is designed for security administrators and security analysts.

Pré-requis

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)

Objectifs

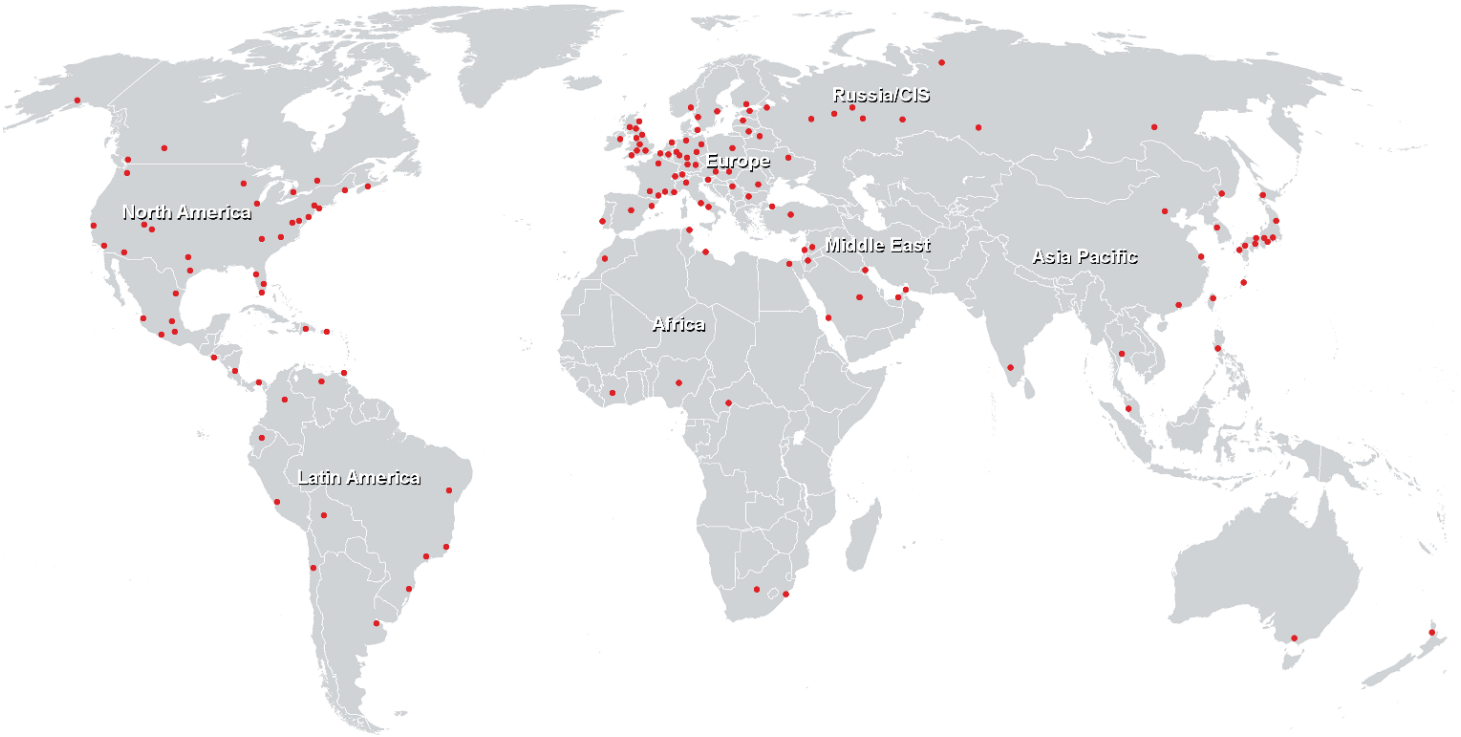
- Learn how to create custom log sources
- Discover how to work with reference data collections and custom rules
- Use X-Force data and Threat Intelligence app
- Use the Use Case Manager app
- Learn how to use UBA and QRadar Advisor
- Discover Tuning
- Explore Custom action scripts
- Discuss Integration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

Contenu

- Unit 1: Custom log sources
- Unit 2: Reference data collections and custom rules
- Unit 3: IBM X-Force Threat Intelligence in QRadar
- Unit 4: User Behavior Analytics and Advisor with Watson
- Unit 5: Tuning
- Unit 6: Custom action scripts
- Unit 7: IBM SOAR integration

IBM QRadar SIEM Advanced Topics (BQ204G)

Centres de formation dans le monde entier





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch