QRadar SOAR: Foundations

Course code: BQ405G

In this course, you learn about the IBM Security® QRadar® SOAR architecture, and how to position the product in your company's security architecture design. You gain hands-on experience with the SOAR interface, by investigating and managing cases and users with the SOAR Breach Response module, playbooks, and email integration.

Who is the course for

- Security operations center (SOC) Administrator
- SOC Analyst
- Security Analyst
- Incident Responder
- Managed Service Security Provider (MSSP)

What we teach you

In this course, you learn about the following topics:

- QRadar SOAR architectural patterns
- Install the product, and configure license and access
- Review the SOAR Console
- Manage cases
- Utilize the concept of artifacts
- Utilize case management capabilities
- Integrate email system for users and case management
- Focus on the Breach Response module
- Gain hands-on experience with the SOAR platform
- Design playbooks
- Integrate IBM and third-party solutions with SOAR

Required skills

- null

Course outline

Getting started

- Describe architectural patterns
- Install the product and configure license and access
- Review the SOAR Console
- Manage cases and use Breach Response add-on
- Utilize the concept of artifacts

Case management and email integration

- Utilize case management capabilities
- Integrate email system for users and case management
- Focus on the Breach Response module

Playbooks and integrations

- Gain hands-on experience with the SOAR platform
- Design playbooks
- Integrate IBM and third-party solutions with SOAR

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk