QRadar SOAR: Foundations

Course Overview

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

Audience

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

Objectives

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

Agenda:

Day 1 – Foundations & Architecture

- Introduction to IBM SOAR
  - What is SOAR and its role in SOC operations
  - SOAR vs SIEM – complementing QRadar
  - SOAR architectural patterns and deployment models
- Installation & Configuration
  - Product installation overview
  - License setup & user access control
  - Role-based access management
- SOAR Console Tour
  - Navigation
  - Dashboards and widgets
  - Core modules overview
- Hands-On Lab: First login, license activation, role creation, console walk-through

Day 2 – Case Management & Artifacts

- Case Management Deep Dive
  - Case creation & lifecycle
  - Assignments, tasks, and evidence
  - Incident severity, categorization, SLAs
- Artifacts
  - Adding and managing artifacts
  - Threat intelligence enrichment
  - Correlating artifacts with external systems
- Breach Response Module
  - Incident response workflow
  - Data breach notifications & compliance tracking
- Hands-On Lab: Create a case, add artifacts, assign tasks, walk through breach response

Day 3 – Integrations & Email System

- Email Integration
  - Configuring email ingestion for case creation
  - Using email for user notifications and approvals
- Third-Party Integrations
  - QRadar SIEM & SOAR integration overview
  - Other IBM integrations (Guardium, MaaS360, etc.)
  - Threat Intel feeds (X-Force Exchange, VirusTotal, etc.)
- REST APIs & Extensions
  - Using REST API for automation
  - App Host and integration server
- Hands-On Lab: Configure email integration, connect SOAR with QRadar & one threat intel feed

Day 4 – Playbooks & Automation

- Playbook Design
  - Playbook editor introduction
  - Event-driven vs manual playbooks
  - Conditional branching, sub-workflows
- Automation with SOAR
  - Scripts and rules
  - Automatic enrichment (IP, Hash, URL lookups)
  - Orchestrating multi-step incident responses
- Best Practices
  - Building reusable playbooks
  - Avoiding common mistakes in automation design
- Hands-On Lab: Build 2 playbooks — malware investigation and phishing response

Day 5 – Advanced Use Cases & Operations

- Complex Playbook Scenarios
  - Integrating multiple data sources (SIEM + Threat Intel + Ticketing)
  - Orchestrating containment with firewalls, EDR, and IAM
- Operationalizing SOAR
  - Metrics & reporting (MTTD, MTTR, SLA tracking)
  - Tuning cases and playbooks to reduce noise
  - SOC use cases & best practices
- SOAR in Real-World Operations
  - Threat hunting & proactive use of SOAR
  - Continuous improvement for IR workflows
- Final Hands-On Workshop
  - End-to-end scenario: Phishing attack → Case creation → Artifact enrichment → Playbook execution → Containment & reporting
- Wrap-Up
  - Key takeaways
  - SOAR roadmap & resources for further learning