IBM SOAR (Resilient) Fundamentals Training

Course code: IBMSOAR1

This Tech Data exclusive training focuses on fundamental knowledge of IBM SOAR (Resilient). The training includes presentation from the trainer as well as excercises in lab environment for better experience in practice.

Who is the course for

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- SIEM basics
- Basic programming concepts

Teaching materials

IBM guide book for this course.

Course outline

Day 1

- What is SOAR, usage, basic working principles, basic functionality
- SOAR Architecture, components and how they interact with each other, typical HW configuration, ports, protocols, On-prem vs. Cloud, HA/DR, integration
- Introduction to GUI
- Administrator settings, users, groups, roles
- Organization, workspaces
- Pre-installed APIs
- Common use cases
- Create and edit Incidents

Day 2

- Incident types, Phases, Tasks
- Defanging URLs, wiki, notifications, search
- Working with Privacy module and Breach notification
- Inbound email processing automation
- Reports and dashboards
- Customization - Fields, Tabs
- Rules, Playbooks, Workflows 1
- Rules, Playbooks, Workflows 2
- Python scripts, functions

Day 3

- Integrations: App Host, App Exchange, SIEM + SOAR
- Incident response automation
- Disaster recovery
- Alternative authentication methods - LDAP, SAML, MFA
- Custom scenarios creation, Q&A
- Foundation training recap, outline of Advanced Training content

GOPAS®