Updated on 04/12/2024

Sign up

# Swimlane Turbine Training SOAR

3 days (21 hours)

## Presentation

Swimline Turbine is an advanced orchestration, automation and incident response (SOAR) solution, offering efficient management of security processes by integrating cybersecurity tools and automating workflows to reduce threat response time.

Our Swimlane Turbine SOAR training course is designed to get you fully operational on the Swimlane platform and to enable you to prove your skills.

This training course will prepare you to effectively manage, automate and orchestrate security processes using Swimlane Turbine, enabling you to respond more quickly and effectively to security incidents in your organization.

This training session will take place on Swimlane version 10.19.

## Objectives

- **Understanding SOAR architecture and concepts**
- Develop the skills needed to mitigate threats and respond to incidents more effectively
- Improve incident management processes

## Target audience

This course is aimed primarily at IT security professionals, such as :

- SOC (Security Operations Center) and SOAR engineers

- Security Analysts
- Security administrators
- Incident management managers
- Cybersecurity consultants
- Risk management professionals

## Prerequisites

- Basic knowledge of cybersecurity, scripting and automation
- Knowledge of security tools
- Understanding of APIs and Webhooks (recommended)

Note: Ambient-IT is not the owner of Swimlane Turbine©, Swimlane Turbine© is a registered trademark of Swimlane©.

# OUR SWIMLANE TURBINE TRAINING PROGRAM

## SWIMLANE INTRODUCTION & CONFIGURATION

- Introduction to Swimlane Turbine
- Overview of SOAR use cases and its role in automating security processes
- License management and configuration
- Appliance installation
- Basic configuration via Web console and command line interface (CLI)
- Appliance update

### COMPONENT AND PLAYBOOK CONFIGURATION

- User profile configuration
- SOAR solution deployment: preparation and prerequisites
- Project scope definition and deployment planning
- Setting up SOAR environments
  - Integration of applications and data sources
  - Creation of enrichment strategies and log processing policies
- Development of playbooks for automating incident response processes

### AUTOMATIZATION AND ORCHESTRATION OF INCIDENTS

- Setting up automated workflows for routine incidents
- Orchestration of security tools
- Creating and managing tasks in playbooks
- Automated incident response: threat identification and management
- Case studies: development of playbooks for typical incidents (phishing, malware)

MANAGEMENT AND OPTIMIZATION

- Advanced architecture
- Workflow and playbook optimization
- User and role management
- Implementing Threat Intelligence in playbooks
- Support, troubleshooting and resolving common problems
- Data security and backup

## Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

## Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level on different types of technology, as well as his or her expectations and personal objectives with regard to the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

## Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

## Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

## Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

## Sanction

A certificate will be issued to each trainee who completes the course.