FortiSOAR Analyst (SOAR-ANL)

ID SOAR-ANL **Price** on request **Duration** 3 days

Who should attend

SOC analysts responsible for developing playbooks; creating modules, templates, dashboards, and widgets; and performing incident handling with FortiSOAR should attend this course.

This course is part of the following Certifications

NSE 6 Certified: Security Operations (NSE6SO)

Prerequisites

You must have an understanding of the topics covered in the FortiOS Administrator course (or have equivalent experience).

It is also recommended that you have an understanding of the topics covered in the following courses, or have equivalent experience:

- FortiManager Administrator (FMG)
- !FortiSOAR Administrator (FORT-SOARADMIN)
- Basic familiarity with Python programming
- Basic familiarity with the Jinja2 templating language
- Basic familiarity with email security and SIEM technology

Course Objectives

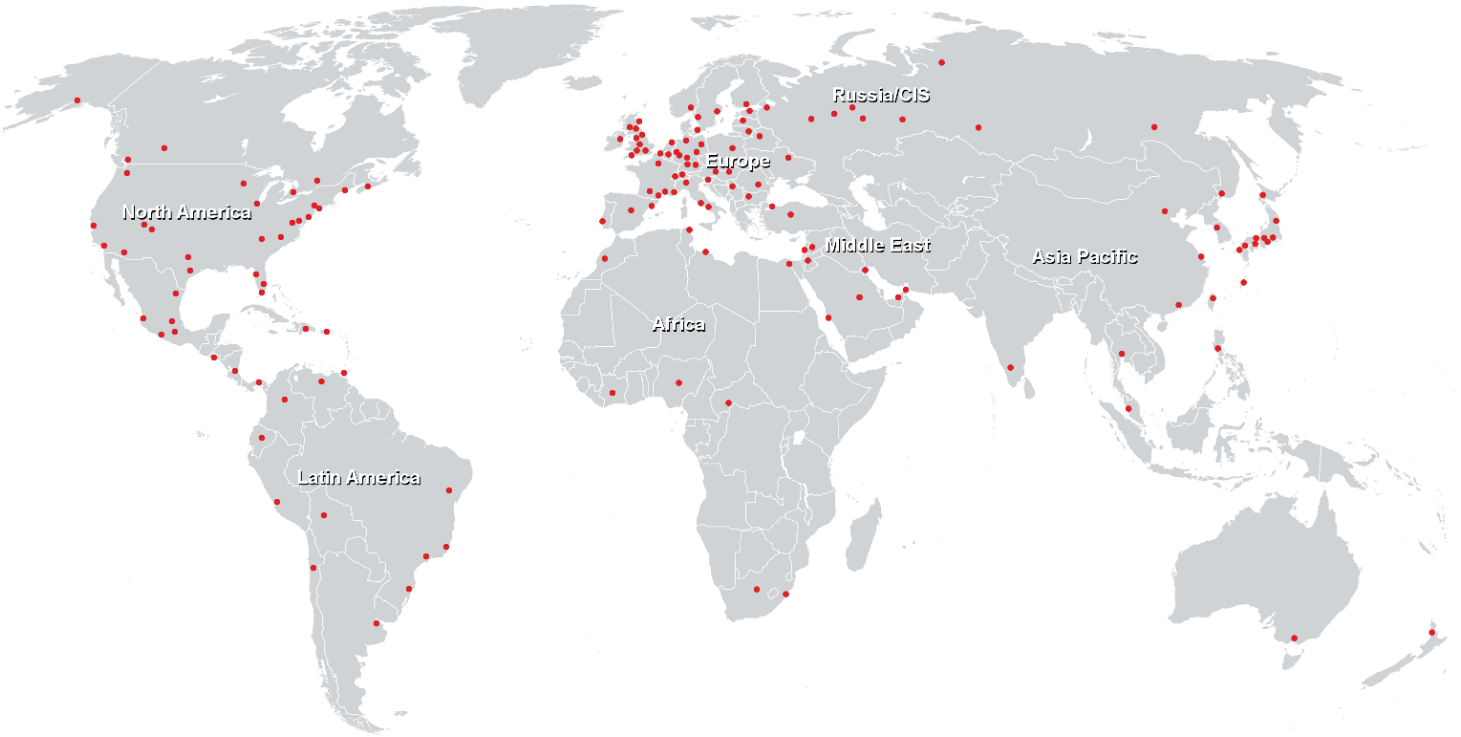
After completing this course, you should be able to:

- Describe SOAR, SIEM, automation, and orchestration
- Describe modules, deployment models, and FortiSOAR device types
- Navigate the FortiSOAR GUI
- Customize navigation with the navigation editor
- Describe the SOAR Framework solution pack
- Describe templates, dashboards, and reports
- Describe security management, role-based access, and teams
- Describe FortiSOAR playbook triggers
- Describe FortiSOAR playbook steps
- Create a playbook
- Ingest data from FortiSIEM
- Create preprocessing rules
- Describe Jinja and JSON, and how FortiSOAR uses them
- Describe dynamic variables and values
- Describe built-in functions
- Design and publish a module
- Export and import FortiSOAR entities
- Configure dashboards
- Configure widgets in templates
- Apply operators to evaluate conditions
- Demonstrate the JSON and YAQL query filters
- Describe FortiSOAR incidents
- Describe campaigns
- Describe the MITRE ATT&CK Matrix for Enterprise
- Describe incident phases on FortiSOAR
- Describe the incident handling workflow on FortiSOAR
- Configure shift and queue management
- Configure war rooms
- Troubleshoot common playbook issues
- Troubleshoot common connector issues
- Configure logging levels and log files for analysis
- Describe API basics
- Configure the FortiSOAR API
- Configure FortiManager API integration with FortiSOAR
- Describe FortiAI on FortiSOAR

Note: This course introduces basic widget and connector folder and file structures. It does not cover the programming required to develop custom widgets and connectors.

FortiSOAR Analyst (SOAR-ANL)

Training Centres worldwide



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