Advanced Analytics (FORT-ADVANALYTICS)

ID FORT-ADVANALYTICS **Price** on request **Duration** 3 days

This training is provided by our partner Fortinet.

Who should attend

Security professionals involved in the management, configuration, administration, and monitoring of FortiSIEM and FortiSOAR devices in an enterprise or service provider deployment used to monitor and secure the networks of customer organizations.

Prerequisites

You must have an understanding of the topics covered in the following courses, or have equivalent experience:

- FortiGate Security (FORT-SECI)
- FortiGate Infrastructure (FORT-INFRA)
- FortiSIEM Analyst (FORT-SIEM)

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

- Python programming
- Jinja2 template language for Python
- Linux systems
- SOAR technologies

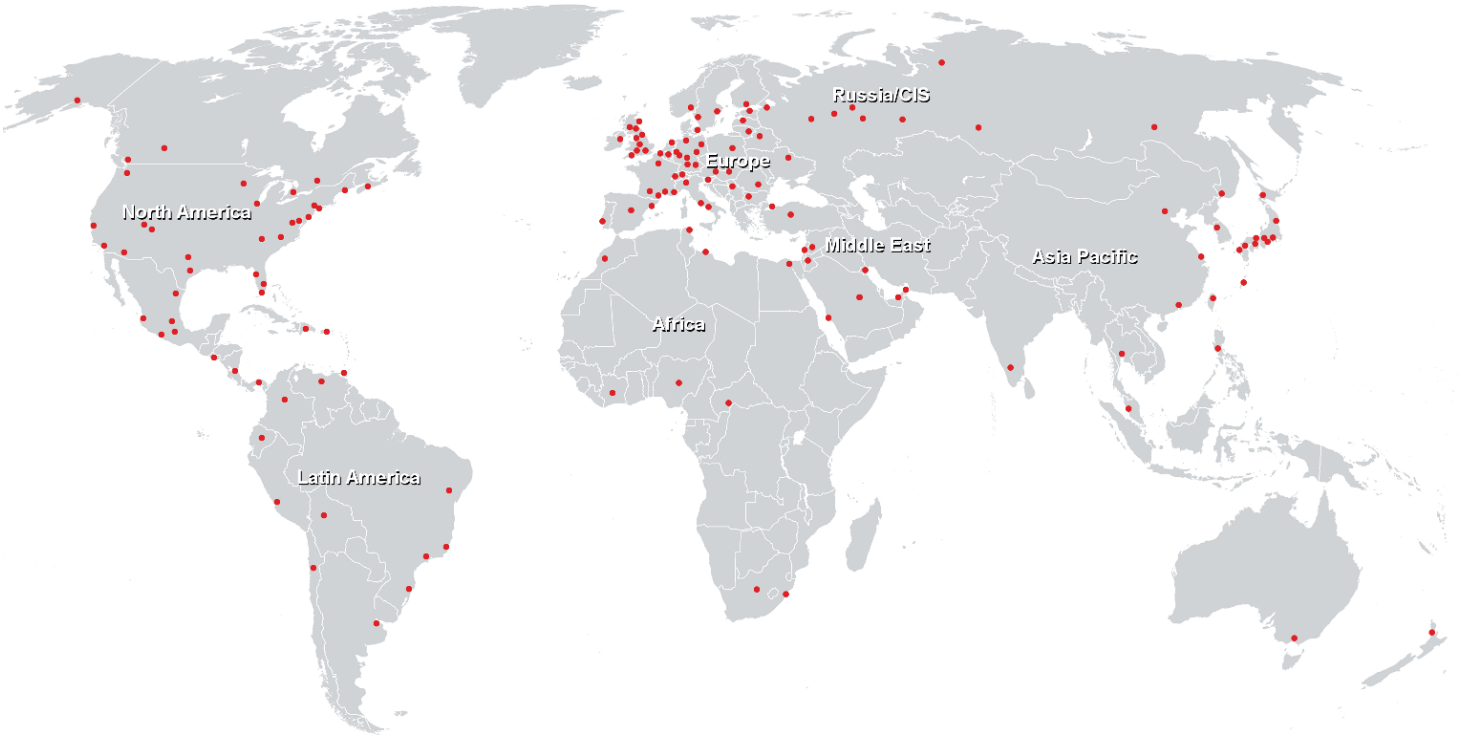
Course Objectives

After completing this course, candidates will be able to:

- Identify various implementation requirements for a multi-tenant FortiSIEM deployment
- Deploy FortiSIEM in a hybrid environment with and without collectors
- Design multi-tenant solutions with FortiSIEM
- Deploy collectors in a multi-tenant environment
- Manage EPS assignment and restrictions on FortiSIEM
- Manage resource utilization of a multi-tenant FortiSIEM cluster
- Maintain and troubleshoot a collector installation
- Deploy and manage Windows and Linux agents
- Create rules by evaluating security events
- Define actions for a single pattern security rule
- Identify multiple pattern security rules and define conditions and actions for them
- Differentiate between a standard and baseline report
- Create your own baseline profiles
- Deploy FortiSIEM UEBA agents
- Examine log-based UEBA rules
- Examine nested queries for advanced analytics
- Configure lookup tables for advanced analytics
- Configure clear conditions on FortiSIEM
- Analyze some out-of-the-box remediation scripts
- Configure various remediation methods on FortiSIEM
- Integrate FortiSOAR with FortiSIEM
- Remediate incidents from FortiSOAR

Advanced Analytics (FORT-ADVANALYTICS)

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