Advanced Analytics (FORT-ADVANALYTICS)

ID FORT-ADVANALYTICS **Prix** sur demande **Durée** 3 jours

A qui s'adresse cette formation

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

Pré-requis

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 (FORT-SIEM)

It is also highly recommended that you have an understanding, or equivalent experience with, Python programming, Jinja2 template language for Python, Linux systems, and SOAR technologies.

System Requirements- If you take the online format of this class, you must use a computer that has the following:

- A high-speed Internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers or headphones

One of the following:

- HTML 5 support OR
- An up-to-date Java Runtime Environment (JRE) with Java Plugin enabled on your web browser

You should use a wired Ethernet connection, not a WiFi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Objectifs

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 the incident attributes that trigger an incident
- Identify multiple pattern security rules and define conditions and actions for them
- Differentiate between a standard and baseline report
- Create your own baseline profiles
- Examine the MITRE ATT&CK framework integration on FortiSIEM and FortiSOAR
- Deploy FortiSIEM UEBA agents
- Examine UEBA rules, reports, event types, and windows template
- 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

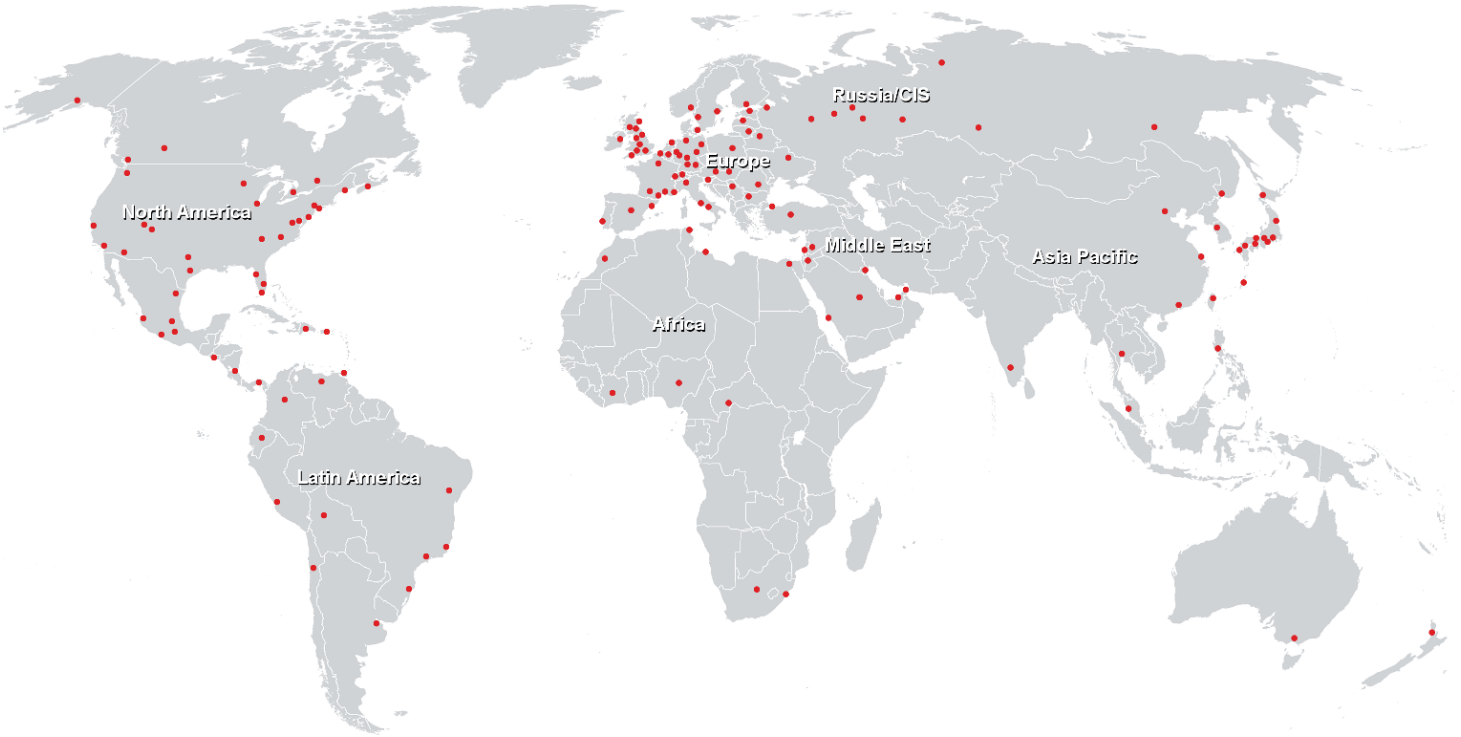
Contenu

- Introduction to Multi-tenancy
- Defining Collectors and Agents
- Operating Collectors
- Windows and Linux Agents
- Rules
- Single Subpattern Security Rule
- Multiple Subpattern Rules
- Introduction to Baseline
- Baseline
- UEBA
- MITRE ATT&CK
- Clear Conditions
- Remediation

Advanced Analytics (FORT-ADVANALYTICS)

Advanced Analytics (FORT-ADVANALYTICS)

Centres de formation dans le monde entier



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