FortiSIEM Analyst (FORT-SIEM)

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

A qui s'adresse cette formation

Security professionals responsible for the detection, analysis, and remediation of security incidents using FortiSIEM should attend this course.

Cette formation prépare à la/aux certifications

NSE 6 Certified: Security Operations (NSE6SO)

Pré-requis

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

- FortiGate Operator
- !

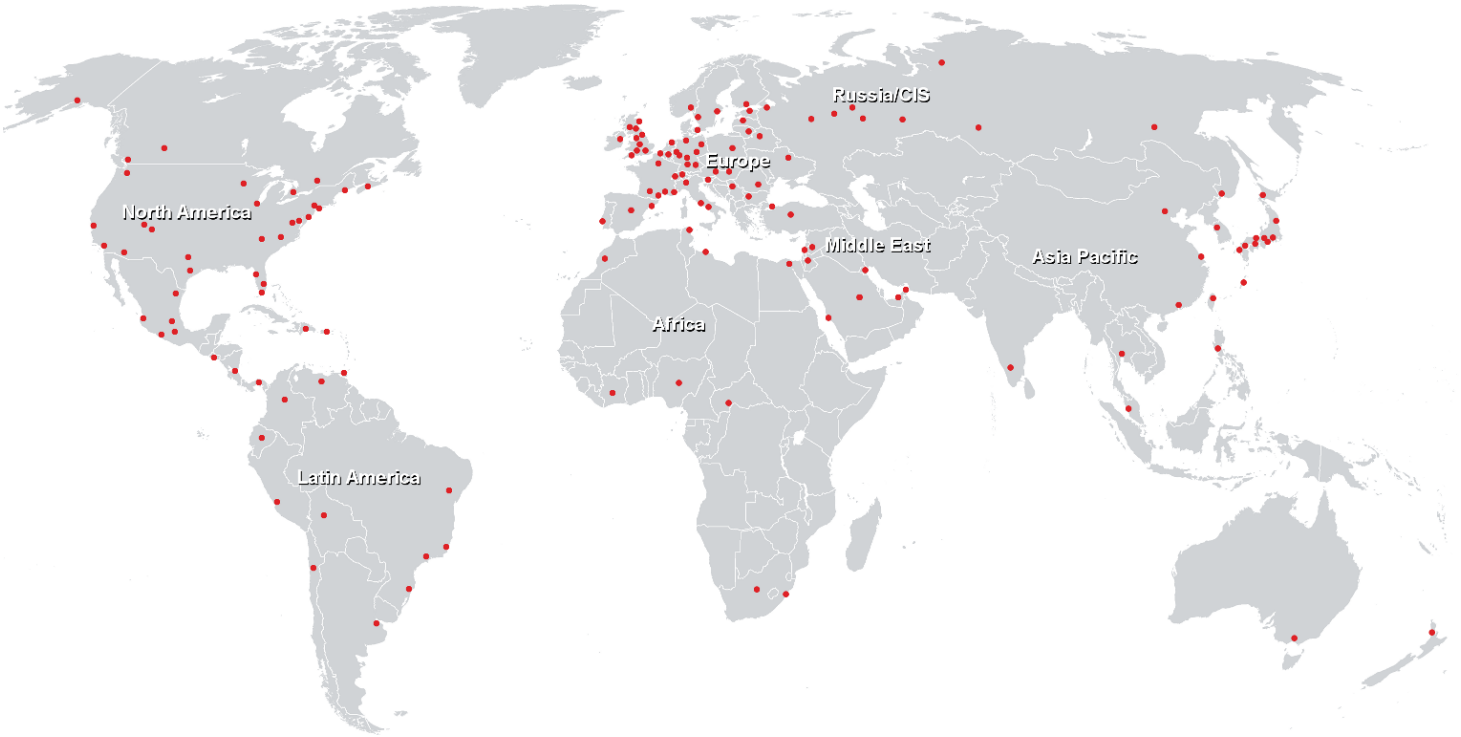
Objectifs

After completing this course, you should be able to:

- Describe how FortiSIEM solves common cybersecurity challenges
- Describe the main components and the unique database architecture on FortiSIEM
- Perform real-time and historical searches
- Define structured search operators and search conditions
- Reference the CMDB data in structured searches
- Configure display fields and columns
- Build queries from search results and events
- Build nested queries and lookup tables
- Build rule subpatterns and conditions
- Manage and tune incidents
- Resolve an incident
- Create time-based and pattern-based clear conditions
- Configure automation policies
- Create rules using baselines
- Analyze anomalies against baselines
- Describe the threat hunting workflow
- Analyze threat hunting dashboards
- Describe FortiSIEM ML modes and algorithms
- Describe how to train an ML model perform an analysis using a ML model
- Describe the benefits of deploying FortiSIEM UEBA
- Configure tags, rules, and incidents using UEBA data
- Describe how ZTNA tags affect the FortiSIEM incident and remediation process
- Configure a ZTNA tag using FortiSIEM to remediate incidents
- Generate and export a report
- Create a custom dashboard

FortiSIEM Analyst (FORT-SIEM)

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