Chronicle SIEM Fundamentals (CSIEMF)

ID CSIEMF **Prix** CHF 2 995,– (Hors Taxe) **Durée** 3 jours

A qui s'adresse cette formation

Individuals who need a basic introduction to Chronicle SIEM

Pré-requis

Basic knowledge about what is SIEM & SOAR

Objectifs

Explore the essentials of Chronicle, a powerful Security Information and Event Management (SIEM) solution offered as a cloud service on the robust Google infrastructure. The Chronicle Fundamentals course provides an in-depth overview of the key functionalities, data analysis capabilities, and security aspects of Chronicle SIEM.

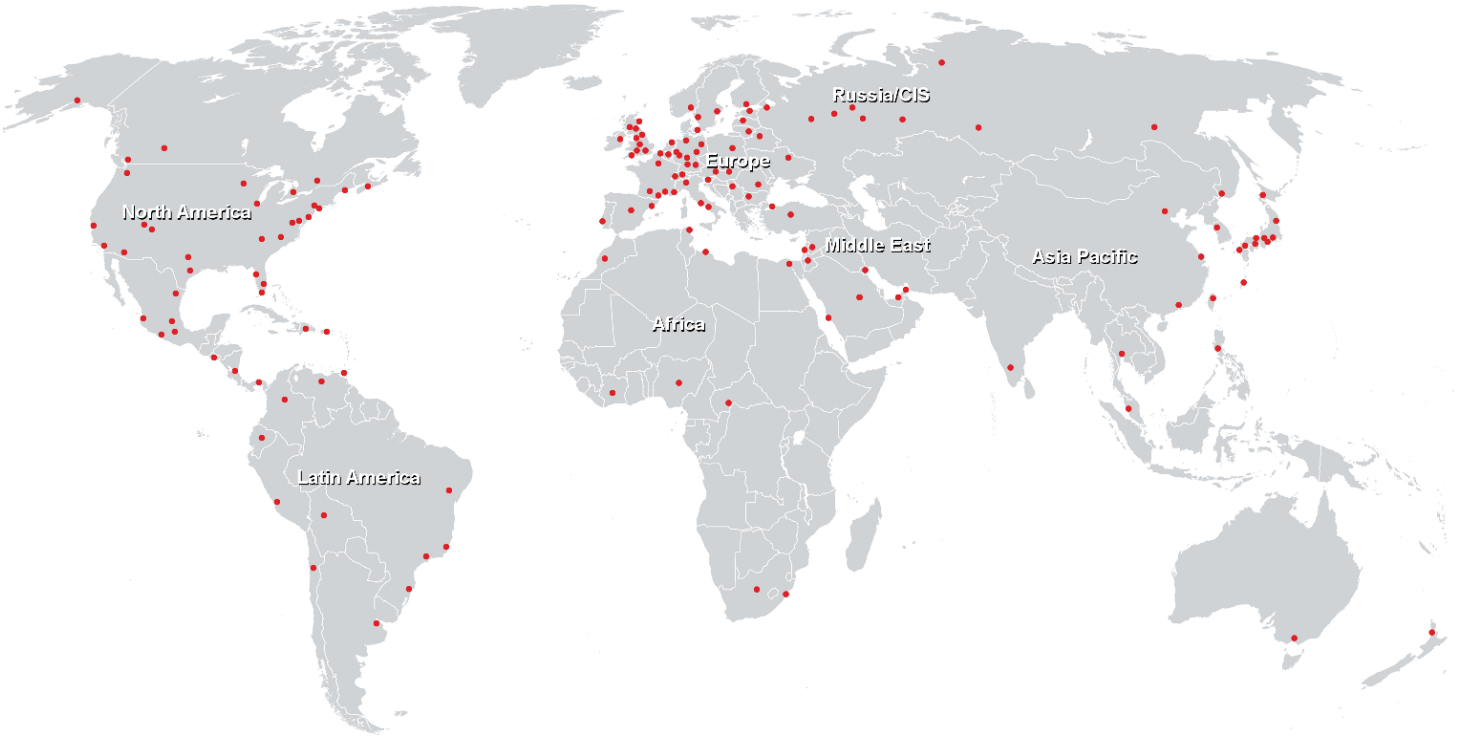
- Chronicle Access – Role-Based Access Control (RBAC) in Chronicle. Why Audit logging is important and how to implement it in your Chronicle instance.
- Learn about Raw Log Search and UDM Search, how to use Search for investigation.
- Chronicle Data On Boarding: forwarders, feed management, ingestion API, and direct ingestion.
- Introduction to Chronicle Parsers – What is a parser, versioning, and parser extension.
- Walkthrough of Chronicle Curated Detection rules.
- Navigating Alerts using the Alert Graph: Entity data, releted alerts, alert context.
- Learn about Entity data – Data enrichment in Chronicle, Entity types (Users & Assets), Resources, Geo IP Enrichment.
- Advanced Search Capabilities: Reference Lists, Group Fields, Pivot, Search for Alerts.
- Parsing data in Chronicle – What are parsers and how can we manage them: Parser update, versioning, parser extensions.
- Building rules for Chronicle: YARA-L 2.0 syntax, Rules UI, Single event rules, Multi-event rules, using entity data in rules, Outcomes, Functions & Lists, best practice.
- Building dashboards in Chronicle.

Contenu

- Module 1: Chronicle Access
- Module 2: Searching with Chronicle
  Hands-On: Raw Log & UDM Search
- Module 3: Chronicle Data On Boarding
  Hands-On: Collect Linux Syslog
- Module 4: Parsing Data In Chronicle
- Module 5: Curated Detections
- Module 6: Visualizing Alerts With Chronicle
  Hands-On: Navigating and Reviewing using Alert Graph
- Module 7: Entity Graph
  Hands-On: Search – Asset\User Enrichment
- Module 8: Advance Searching With Chronicle
  Hands-On: Advanced Search
- Module 9: Building Rules For Chronicle
  Hands-On: Building Rules
- Module 10: Visualizing Alerts (Advance)
- Module 11: Entity Graph (Advance)
- Module 12: Visualizing Data in Chronicle Hands-On: Building Dashboard In Chronicle

Chronicle SIEM Fundamentals (CSIEMF)

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