Chronicle SIEM Fundamentals (CSIEMF)

ID CSIEMF **Preis** auf Anfrage **Dauer** 3 Tage

Zielgruppe

Personen, die eine grundlegende Einführung in Chronicle SIEM benötigen

Voraussetzungen

Grundlegende Kenntnisse darüber, was SIEM und SOAR sind

Kursziele

Lernen Sie die Grundlagen von Chronicle kennen, einer leistungsstarken SIEM-Lösung (Security Information and Event Management), die als Cloud-Service auf der robusten Google-Infrastruktur angeboten wird. Der Kurs "Chronicle Fundamentals" bietet einen detaillierten Überblick über die wichtigsten Funktionen, Datenanalysemöglichkeiten und Sicherheitsaspekte von Chronicle SIEM.

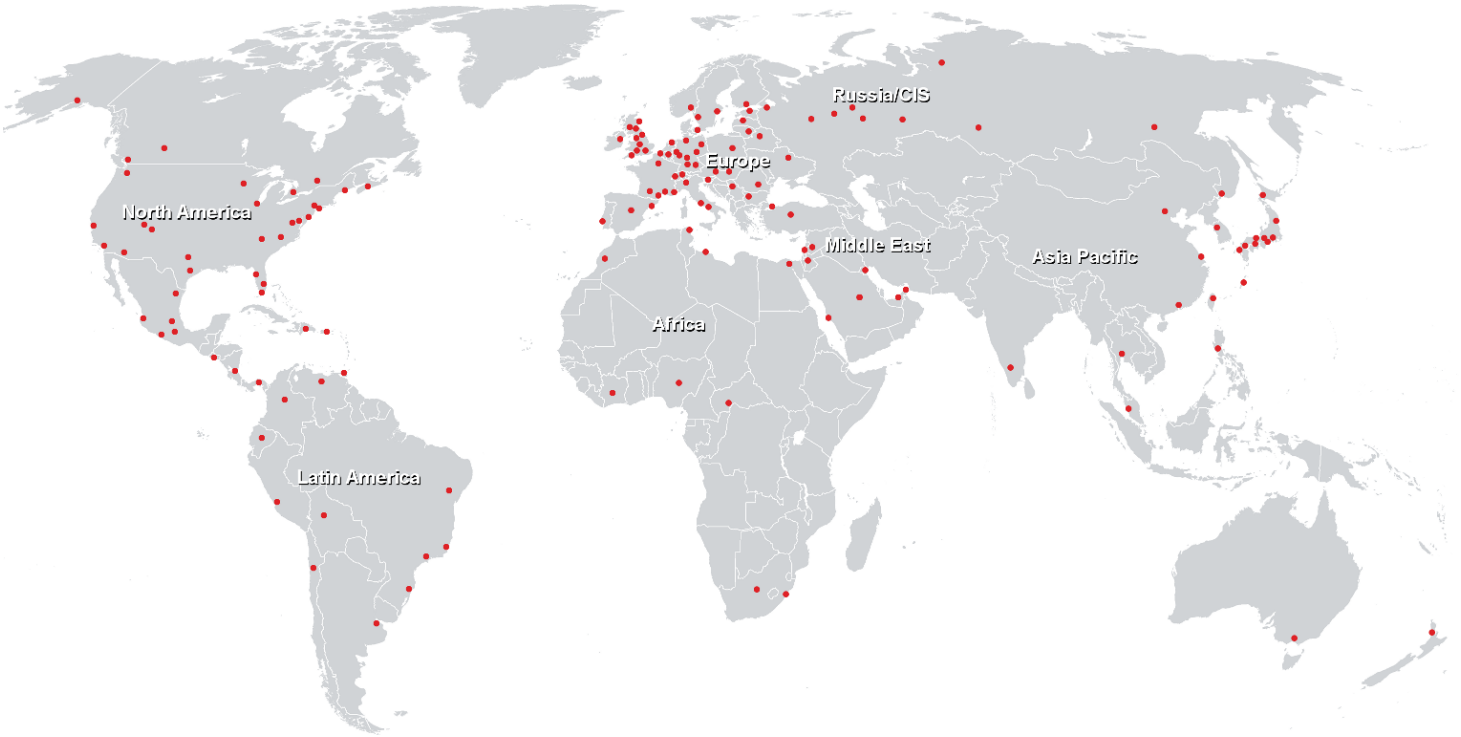
- Chronicle Access - Rollenbasierte Zugriffskontrolle (RBAC) in Chronicle. Warum Audit-Logging wichtig ist und wie Sie es in Ihrer Chronicle-Instanz implementieren.
- Erfahren Sie mehr über die Raw-Log-Suche und die UDM-Suche und wie Sie die Suche für Untersuchungen nutzen können.
- Chronicle Data On Boarding: Forwarder, Feed Management, Ingestion API und direkte Ingestion.
- Einführung in Chronicle Parsers - Was ist ein Parser, Versionierung und Parser-Erweiterung.
- Durchgehender Überblick über die Regeln der Chronicle Curated Detection.
- Navigieren in Warnmeldungen mit Hilfe des Warndiagramms: Entitätsdaten, gelöschte Warnungen, Warnungskontext.
- Erfahren Sie mehr über Entitätsdaten - Datenanreicherung in Chronicle, Entitätstypen (Benutzer & Assets), Ressourcen, Geo IP Enrichment.
- Erweiterte Suchfunktionen: Referenzlisten, Gruppenfelder, Pivot, Suche nach Warnungen.
- Parsing von Daten in Chronicle - Was sind Parser und wie können wir sie verwalten: Parser-Aktualisierung, Versionierung, Parser-Erweiterungen.
- Erstellen von Regeln für Chronicle: YARA-L 2.0-Syntax, Regel-UI, Einzelereignisregeln, Multi-Ereignisregeln, Verwendung von Entitätsdaten in Regeln, Ergebnisse, Funktionen & Listen, Best Practice.
- Erstellung von Dashboards in Chronicle.

Kursinhalt

- Modul 1: Zugang zur Chronik
- Modul 2: Suche mit Chronicle
  Hands-On: Raw Log & UDM Search
- Modul 3: Chronikdaten an Bord
  Hands-On: Linux Syslog sammeln
- Modul 4: Parsing von Daten in der Chronik
- Modul 5: Kuratierte Erkennungen
- Modul 6: Visualisierung von Alarmen mit Chronicle
  Praktische Übungen: Navigieren und Überprüfen mit Alert Graph
- Module 7: Entity Graph
  Hands-On: Search – Asset\User Enrichment
- Modul 8: Erweiterte Suche mit Chronicle
  Hands-On: Erweiterte Suche
- Modul 9: Regeln für die Chronik erstellen
  Praktische Übungen: Regeln erstellen
- Modul 10: Visualisierung von Alarmen (Fortgeschrittene)
- Modul 11: Entitätsdiagramm (Fortgeschrittene)
- Modul 12: Visualisierung von Daten in Chronicle Praktische Übungen: Erstellung eines Dashboards in Chronicle

Chronicle SIEM Fundamentals (CSIEMF)

Weltweite Trainingscenter



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