Agent Platform and Generative AI Security (VAIGAS)

ID VAIGAS **Preis** CHF 1'500.– (exkl. MwSt.) **Dauer** 2 Tage

Zielgruppe

KI-Praktiker, Sicherheitsexperten und Cloud-Architekten

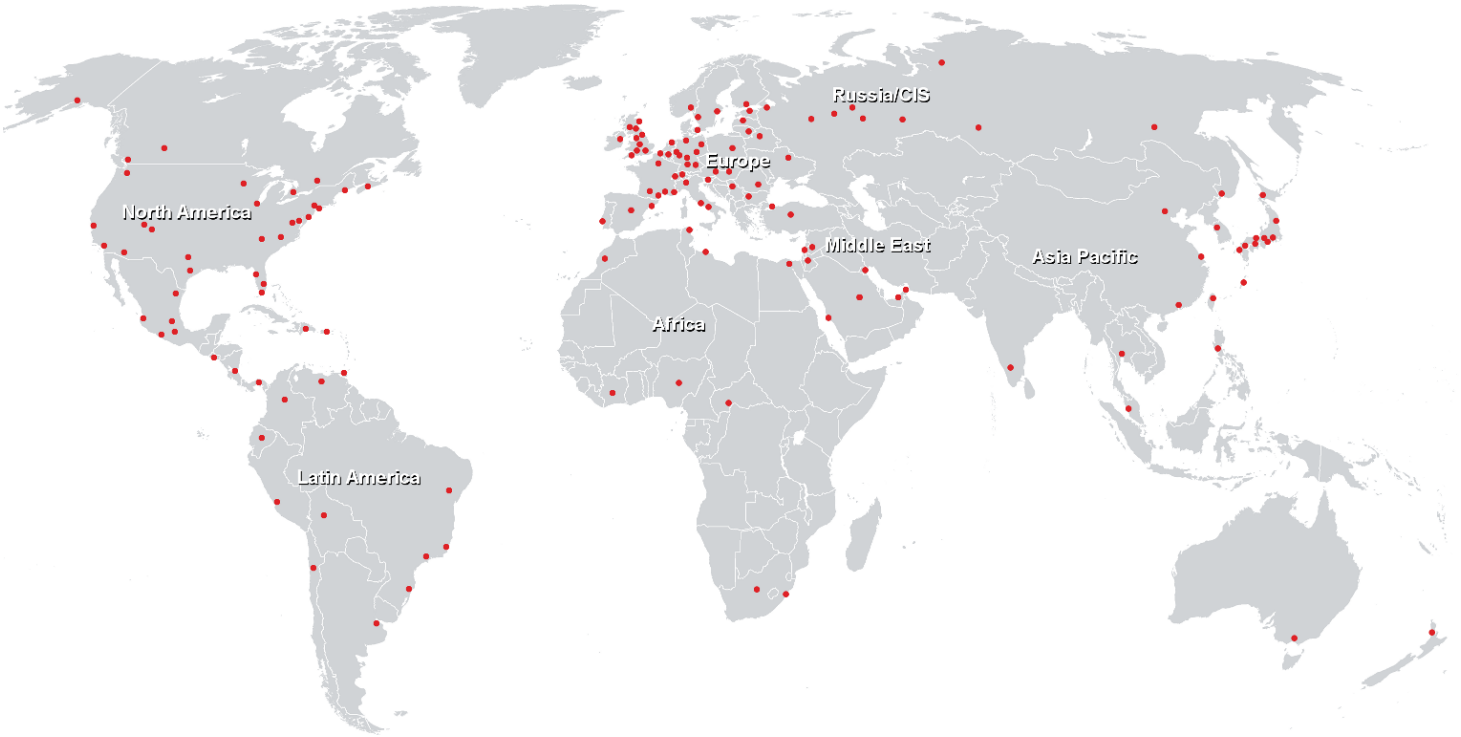
Voraussetzungen

Grundkenntnisse im Bereich maschinelles Lernen, insbesondere generative KI, sowie ein grundlegendes Verständnis der Sicherheit in Google Cloud.

Kursziele

- Grundlegende Kenntnisse über die Agent-Plattform und die damit verbundenen Sicherheitsherausforderungen erwerben.
- Führen Sie Massnahmen zur Identitäts- und Zugriffskontrolle ein, um den Zugriff auf die Ressourcen der Agent-Plattform einzuschränken.
- Konfigurieren Sie Verschlüsselungsstrategien und schützen Sie vertrauliche Informationen.
- Aktivieren Sie Protokollierung, Überwachung und Benachrichtigungen für eine Echtzeit-Sicherheitsüberwachung des Betriebs der Agent-Plattform.
- Spezifische Sicherheitsrisiken im Zusammenhang mit generativer KI identifizieren und mindern.
- Wenden Sie Testverfahren an, um die Antworten generativer KI-Modelle zu validieren und deren Sicherheit zu gewährleisten.
- Setzen Sie bewährte Verfahren zur Sicherung von Datenquellen und Antworten in RAG-Systemen (Retrieval-Augmented Generation) um.
- Grundlegende Kenntnisse zum Thema KI-Sicherheit erwerben.

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