Vertex AI and Generative AI Security (VAIGAS)

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

Zielgruppe

KI-Fachleute, Sicherheitsexperten und Cloud-Architekten

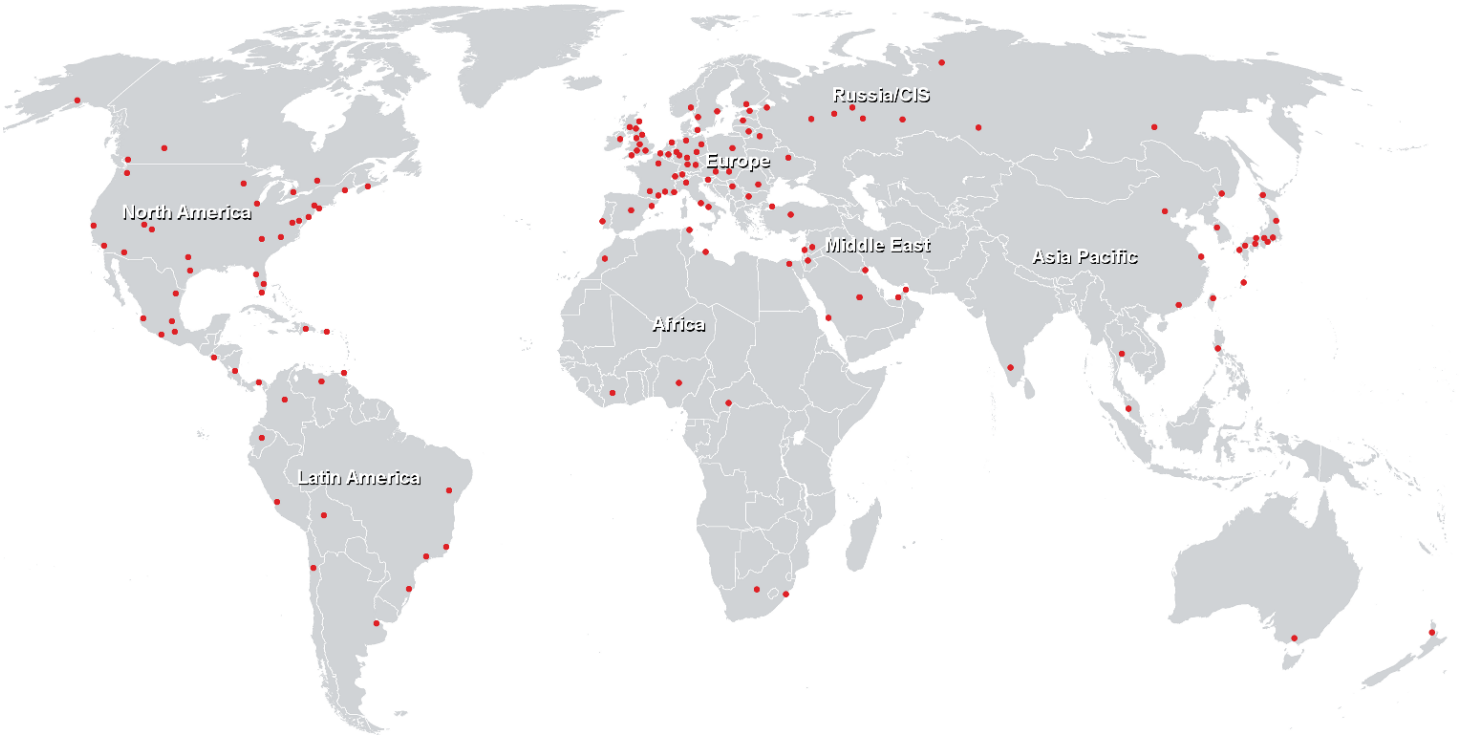
Voraussetzungen

Grundlegende Kenntnisse des maschinellen Lernens, insbesondere der generativen KI, und Grundkenntnisse der Sicherheit in der Google Cloud.

Kursziele

- Aufbau von Grundkenntnissen über Vertex AI und die damit verbundenen Sicherheitsherausforderungen.
- Implementierung von Massnahmen zur Identitäts- und Zugangskontrolle, um den Zugang zu Vertex AI-Ressourcen zu beschränken.
- Konfigurieren Sie Verschlüsselungsstrategien und schützen Sie sensible Informationen.
- Aktivieren Sie die Protokollierung, Überwachung und Alarmierung für die Echtzeit-Sicherheitsüberwachung von Vertex AI-Operationen.
- Identifizierung und Entschärfung einzigartiger Sicherheitsbedrohungen im Zusammenhang mit generativer KI.
- Anwendung von Testtechniken zur Validierung und Absicherung von generativen KI-Modellantworten.
- Implementierung von Best Practices zur Sicherung von Datenquellen und Antworten in Retrieval-Augmented Generation (RAG)-Systemen.
- Aufbau von Grundkenntnissen über KI-Sicherheit.

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