

Govern agents on Gemini Enterprise Agent Platform (GAGEAP)

ID GAGEAP Preis CHF 350.— (exkl. MwSt.) Dauer 4 Stunden

Zielgruppe

Architekten, Cloud-Entwickler, KI-Ingenieure, Sicherheitsexperten.

Voraussetzungen

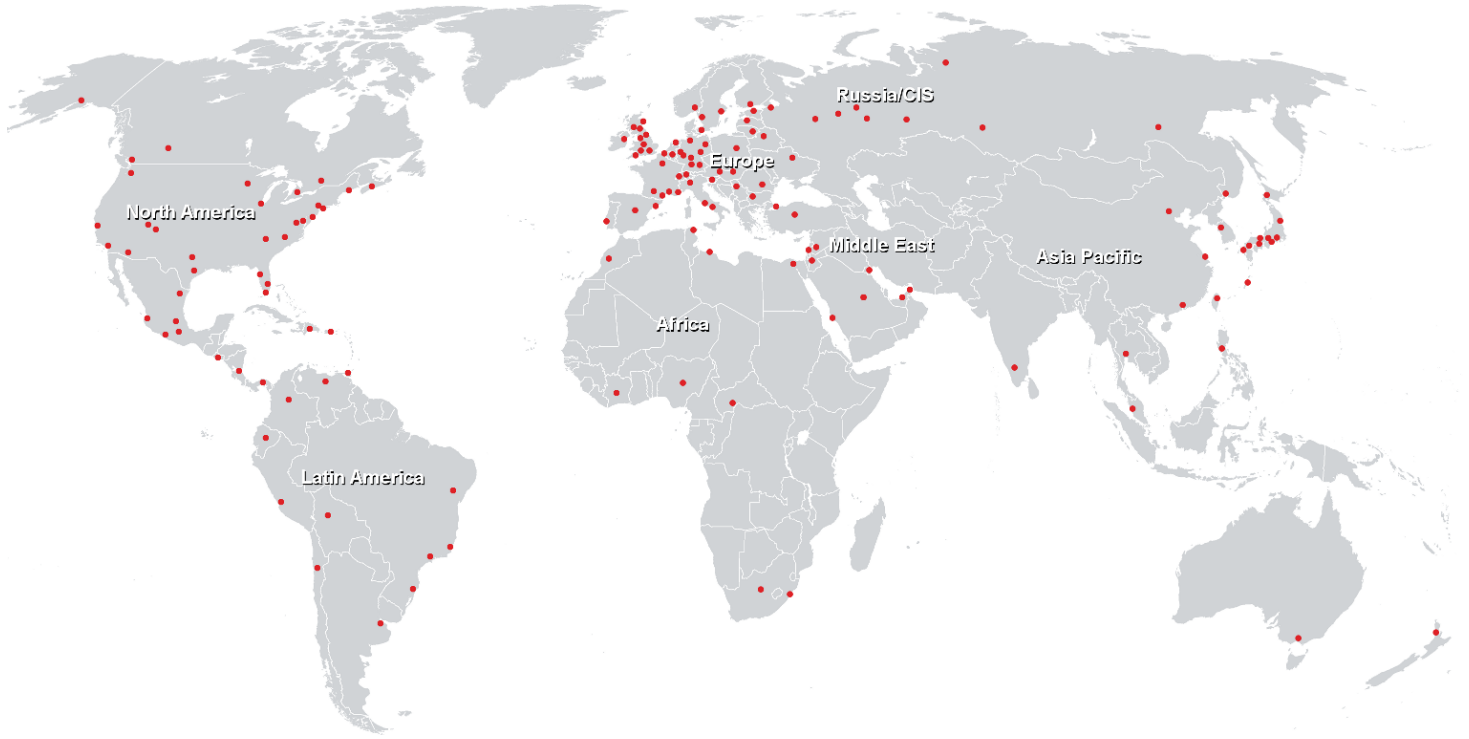
Praktische Kenntnisse in der Erstellung von ADK-Agenten und deren Bereitstellung in der Agent Runtime.

Kursziele

- Setzen Sie Agent Gateway als zentrale Lösung für die Verwaltung der Netzwerk- und Inhaltssicherheit ein.
- Implementieren Sie Sicherheitsmassnahmen für Inhalte mithilfe von Model Armor und Cloud DLP, um semantische Bedrohungen wie Prompt-Injection und Datenlecks zu minimieren.
- Richten Sie einen Zero-Trust-Sicherheitsperimeter ein, indem Sie eine eindeutige Agent-Identität mit mTLS, eine toolbezogene Autorisierung mit REQUEST_AUTHZ und detaillierte CEL-Richtlinien nutzen.
- Entdecken Sie Agent-Tools über das Agent Registry und sorgen Sie mithilfe von Cloud Trace und dem Security Command Center für durchgängige Überwachbarkeit und Bedrohungserkennung.



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>