

---

## Vertex AI and Generative AI Security (VAIGAS)

ID VAIGAS Price on request Duration 2 days

### Who should attend

AI practitioners, security professionals, and cloud architects

### Prerequisites

Fundamental knowledge of machine learning, in particular generative AI, and basic understanding of security on Google Cloud.

### Course Objectives

- Establish foundational knowledge of Vertex AI and its security challenges.
- Implement identity and access control measures to restrict access to Vertex AI resources.
- Configure encryption strategies and protect sensitive information.
- Enable logging, monitoring, and alerting for real-time security oversight of Vertex AI operations.
- Identify and mitigate unique security threats associated with generative AI.
- Apply testing techniques to validate and secure generative AI model responses.
- Implement best practices for securing data sources and responses within Retrieval-Augmented Generation (RAG) systems.
- Establish foundational knowledge of AI Safety.

## Training Centres worldwide



## Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3  
CH-8304 Wallisellen  
Tel. +41 44 832 50 80

[info@flane.ch](mailto:info@flane.ch), <https://www.flane.ch>