Agent Platform and Generative AI Security (VAIGAS)

ID VAIGAS **Prix** CHF 1 500,– (Hors Taxe) **Durée** 2 jours

A qui s'adresse cette formation

Praticiens de l'IA, professionnels de la sécurité et architectes cloud

Pré-requis

Connaissances fondamentales en apprentissage automatique, en particulier en IA générative, et compréhension de base de la sécurité sur Google Cloud.

Objectifs

A l'issue de la formation, vous devrez être en mesure de :

- Avoir des connaissances de base sur Vertex AI et ses enjeux de sécurité.
- Mettre en œuvre des mesures de contrôle d'identité et d'accès pour restreindre l'accès aux ressources Vertex AI.
- Configurer des stratégies de chiffrement et protéger les informations sensibles.
- Activer la journalisation, la supervision et les alertes pour une surveillance en temps réel des opérations Vertex AI.
- Identifier et atténuer les menaces de sécurité spécifiques à l'IA générative.
- Appliquer des techniques de test pour valider et sécuriser les réponses des modèles d'IA générative.
- Mettre en œuvre les bonnes pratiques pour sécuriser les sources de données et les réponses dans les systèmes RAG (Retrieval-Augmented Generation).
- Avoir des connaissances fondamentales sur la sécurité de l'IA.

Contenu

Module 01 - Introduction aux principes de sécurité de Vertex AI

Sujets

- Sécurité sur Google Cloud
- Composants de Vertex AI
- Enjeux de sécurité de Vertex AI

Activités

- Lab : Vertex AI : Entraînement et déploiement d'un modèle personnalisé

Module 02 - Gestion des identités et des accès (IAM) dans Vertex AI

Sujets

- Présentation d'IAM dans Google Cloud

Activités

- Lab : Comptes de service et rôles : fondamentaux

Module 03 - Sécurité des données et confidentialité

Sujets

- Chiffrement des données
- Protection des données sensibles
- Contrôles de service VPC
- Planification de la reprise après sinistre

Activités

- Lab : Premiers pas avec Cloud KMS
- Lab : Création d'une copie désidentifiée de données dans Cloud Storage

Module 04 - Sécurisation des points de terminaison Vertex AI et déploiement de modèles

Sujets

- Sécurité réseau
- Sécurisation des points de terminaison des modèles

Activités

- Lab : Configuration de l'accès privé à Google et de Cloud

NAT

Module 05 - Supervision et journalisation dans Vertex AI

Sujets

- Journalisation
- Supervision

Module 06 - Risques de sécurité dans les applications d'IA générative

Sujets

- Aperçu des risques de sécurité liés à l'IA générative
- Aperçu de la sécurité de l'IA
- Sécurité des invites
- Mécanismes de protection des LLM

Activités

- Lab : Sécurisation avec l'API Vertex AI Gemini
- Lab : Sécurité Gen AI & LLM pour les développeurs

Module 07 - Test et évaluation des réponses de modèles d'IA générative

Sujets

- Test des réponses des modèles d'IA générative
- Évaluation des réponses
- Ajustement fin des LLM

Activités

- Lab : Mesurer les performances Gen AI avec le service d'évaluation de l'IA générative
- Lab : Tests unitaires d'applications d'IA générative

Module 08 - Sécurisation des systèmes RAG (Retrieval-Augmented Generation)

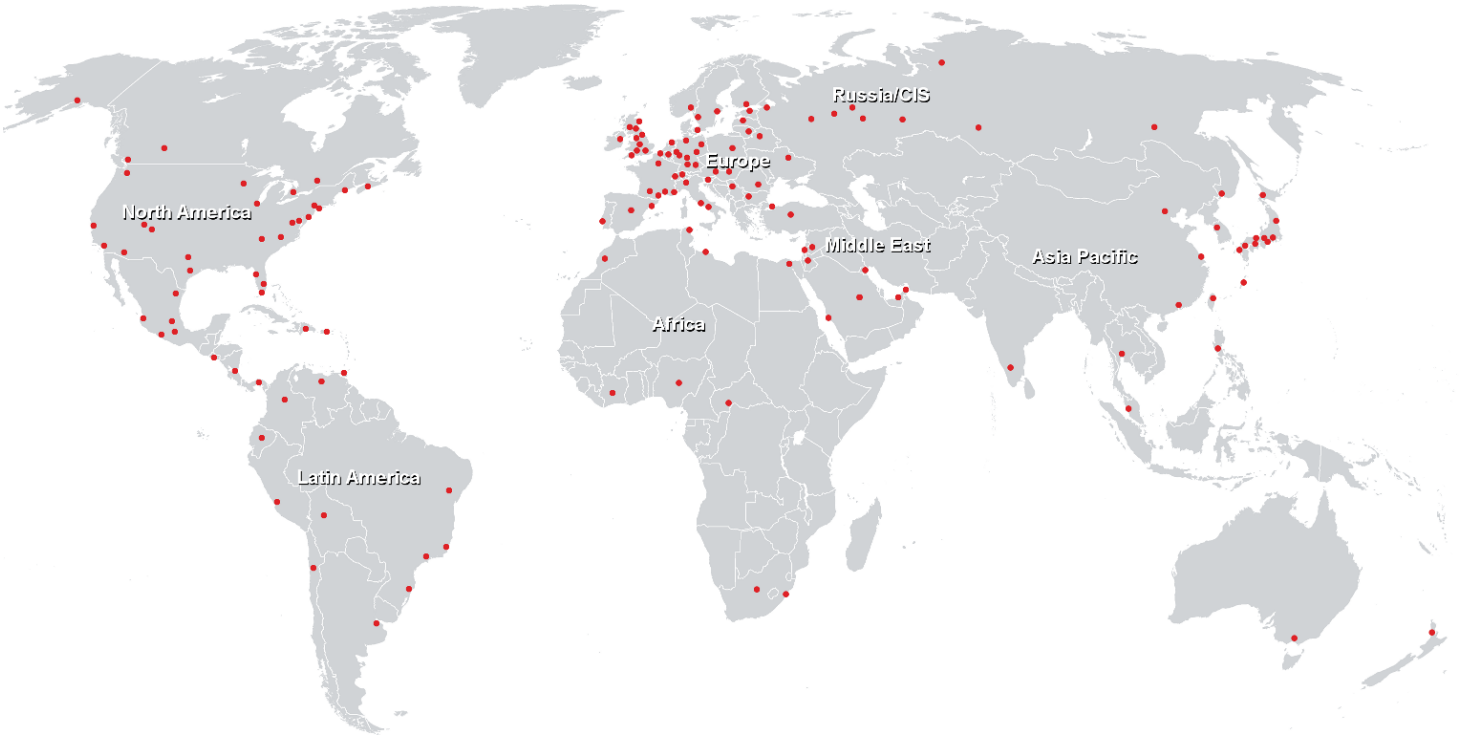
Sujets

- Principes de base de la génération augmentée par récupération
- Sécurité dans les systèmes RAG

Activités

- Lab : RAG multimodal avec l'API Vertex AI Gemini
- Lab : Introduction à l'appel de fonctions avec Gemini

Centres de formation dans le monde entier





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