

## Sécurité de Vertex AI et de l'IA Générative

**Durée: 2 Jours**    **Réf de cours: GO8336**

### Résumé:

Ce cours est conçu pour permettre à votre organisation d'exploiter pleinement le potentiel transformateur des technologies Vertex AI et d'IA générative (gen AI) de Google, avec un fort accent sur la sécurité. Conçu pour les praticiens de l'IA et les ingénieurs en sécurité, il fournit des connaissances ciblées et des compétences pratiques pour naviguer et adopter l'IA de manière sûre et efficace. Les participants acquerront des connaissances pratiques et développeront une approche soucieuse de la sécurité, garantissant une intégration sécurisée et responsable de l'IA générative au sein de leur organisation.

Mise à jour : 26/08/2026

### Public visé:

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

### Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Passer en revue les fondamentaux de la sécurité de Google Cloud.
- Établir une compréhension fondamentale de Vertex AI.
- Énumérer les préoccupations de sécurité liées aux fonctionnalités et composants de Vertex AI
- Contrôler l'accès avec la Gestion des Identités et des Accès.
- Simplifier les permissions en utilisant les hiérarchies et les politiques de l'organisation.
- Utiliser des comptes de service pour un accès au moindre privilège.
- Configurer le chiffrement au repos et en transit.
- Chiffrer les données à l'aide de clés de chiffrement gérées par le client.
- Protéger les données sensibles à l'aide du service de prévention de la perte de données.
- Empêcher l'exfiltration de données à l'aide des contrôles de service VPC.
- Concevoir des systèmes en tenant compte de la reprise après sinistre.
- Déployer des modèles ML à l'aide de points de terminaison de modèle.
- Sécuriser les points de terminaison de modèle.
- Écrire et analyser des journaux.
- Configurer la surveillance et les alertes.
- Identifier les risques de sécurité spécifiques aux LLM et aux applications d'IA générative.
- Comprendre les méthodes pour atténuer les attaques de piratage et d'injection de prompt.
- Explorer les fondamentaux de la sécurisation des modèles et applications d'IA générative.
- Introduire les fondamentaux de la sécurité de l'IA.
- Mettre en œuvre les meilleures pratiques pour tester les réponses des modèles.
- Appliquer des techniques pour améliorer la sécurité des réponses dans les applications d'IA générative.
- Comprendre l'architecture RAG et ses implications en matière de sécurité.
- Mettre en œuvre les meilleures pratiques pour l'ancrage et la sécurisation des sources de données dans les systèmes RAG.

### Pré-requis:

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

### Test et certification

Aucun

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

Aucun

## Contenu:

Module 01 : Introduction aux principes de sécurité de Vertex AI

- Sécurité de Google Cloud
- Composants de Vertex AI
- Préoccupations de sécurité de Vertex AI
- Lab : Vertex AI : Entraînement et service d'un modèle personnalisé

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

- Aperçu d'IAM dans Google Cloud
- Lab : Comptes de service et rôles : Fondamentaux

Module 03 : Sécurité et confidentialité des données

- Chiffrement des données
- Protection des données sensibles
- Contrôles de service VPC
- Planification de la reprise après sinistre
- Lab : Démarrer avec Cloud KMS-
- Lab : Créer une copie désidentifiée des données dans Cloud Storage

Module 04 : Sécurisation des points de terminaison Vertex AI et du déploiement de

modèles

- Sécurité du réseau
- Sécurisation des points de terminaison de modèle
- Lab : Configuration de l'accès privé à Google et de Cloud NAT

Module 05 : Surveillance et journalisation dans Vertex AI

- Journalisation
- Surveillanc

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

- Aperçu des risques de sécurité de l'IA générative
- Aperçu de la sécurité de l'IA
- Sécurité des prompts- Protections des LL
- Lab : Protection avec l'API Vertex AI Gemini
- Lab : Sécurité de l'IA générative et des LLM pour les développeurs

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

- Test des réponses des modèles d'IA générative.
- Évaluation des réponses des modèles.
- Affinage (Fine-tuning) des LLM
- Lab : Mesurer la performance de l'IA générative avec le service d'évaluation de l'IA générative
- Lab : Test unitaire des applications d'IA générative

Module 08 : Sécurisation des systèmes de Génération Augmentée par Récupération (RAG)

- Fondamentaux de la Génération Augmentée par Récupération
- Sécurité dans les systèmes RAG
- Lab : Génération Augmentée par Récupération Multimodale (RAG) avec l'API Vertex AI Gemini
- Lab : Introduction à l'appel de fonction avec Gemini

## Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

### Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "booking form" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via [moncompteformation.gouv.fr](https://moncompteformation.gouv.fr).

### Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur [globalknowledge.fr/handicap](https://globalknowledge.fr/handicap)
- Le Règlement intérieur est disponible sur [globalknowledge.fr/reglement](https://globalknowledge.fr/reglement)