

Vertex AI and Generative AI Security

Formation Sécurité Vertex AI & Gen AI : maîtrisez l'IA générative de Google avec un focus sécurité, pour une adoption sûre et responsable en entreprise

2 jours / 14h

Objectifs pédagogiques

- Établir une connaissance fondamentale de Vertex AI et de ses défis en matière de sécurité.
- Mettre en œuvre des mesures de contrôle d'identité et d'accès pour restreindre l'accès aux ressources de Vertex AI.
- Configurer des stratégies de chiffrement et protéger les informations sensibles.
- Activer la journalisation, la surveillance et les alertes pour une supervision de la sécurité en temps réel des opérations de Vertex AI.
- Identifier et atténuer les menaces de sécurité uniques associées à l'IA générative.
- Appliquer des techniques de test pour valider et sécuriser les réponses des modèles d'IA générative.
- Mettre en œuvre les meilleures pratiques pour sécuriser les sources de données et les réponses dans les systèmes de Génération Augmentée par Récupération (RAG).
- Établir une connaissance fondamentale de la Sécurité de l'IA

Modalités d'évaluation : Les objectifs pédagogiques sont évalués à travers la réalisation des parties pratiques (labs dirigés) sous la supervision du formateur délivrant la session de formation.

Public cible

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

Prérequis

Connaissance fondamentale du Machine Learning, en particulier de l'IA générative, et compréhension de base de la sécurité sur Google Cloud.

Programme

Module 01 : Introduction aux principes de sécurité de Vertex AI

Sujets

- Sécurité de Google Cloud
- Composants de Vertex AI
- Problématiques de sécurité de Vertex AI

Objectifs

- Revoir les fondamentaux de la sécurité de Google Cloud.
- Établir une compréhension fondamentale de Vertex AI.
- Énumérer les problématiques de sécurité liées aux fonctionnalités et composants de Vertex AI.

Activités

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

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

Sujets

- Présentation de l'IAM dans Google Cloud

Objectifs

- Contrôler l'accès avec la Gestion des Identités et des Accès.
- Simplifier les autorisations en utilisant les hiérarchies et les politiques de l'organisation.
- Utiliser les comptes de service pour un accès au moindre privilège.

Activités

- Lab : Comptes de service et rôles : fondamentaux

Module 03 : Sécurité et confidentialité des données

Sujets

- Chiffrement des données
- Protection des données sensibles
- VPC Service Controls
- Planification de la reprise après sinistre

Objectifs

- 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 VPC Service Controls.
- Concevoir des systèmes en tenant compte de la reprise après sinistre

Activités

- Lab : Démarrer avec Cloud KMS
- Lab : Créer une copie dépersonnalisée des données dans Cloud Storage

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

Sujets

- Sécurité réseau
- Sécurisation des points de terminaison de modèle

Objectifs

- Déployer des modèles de ML à l'aide de points de terminaison de modèle.
- Sécuriser les points de terminaison de modèle.

Activités

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

Module 05 : Surveillance et journalisation dans Vertex AI

Sujets

- Journalisation
- Surveillance

Objectifs

- Écrire et analyser les journaux.
- Mettre en place la surveillance et les alertes.

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

Sujets

- Aperçu des risques de sécurité de l'IA générative
- Aperçu de la Sûreté de l'IA
- Sécurité des prompts
- Protections des LLM

Objectifs

- Identifier les risques de sécurité spécifiques aux LLM et aux applications d'IA générative.
- Comprendre les méthodes pour atténuer le piratage des prompts et les attaques par injection.
- Explorer les fondamentaux de la sécurisation des modèles et applications d'IA générative.
- Introduire les fondamentaux de la Sûreté de l'IA.

Activités

- 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

Sujets

- Test des réponses des modèles d'IA générative.
- Évaluation des réponses des modèles.
- Affinage (Fine-tuning) des LLM.

Objectifs

- 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

Activités

- Lab : Mesurer la performance de l'IA générative avec le service d'évaluation de l'IA générative
- Lab : Tests unitaires des applications d'IA générative

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

Sujets

- Fondamentaux de la Génération Augmentée par Récupération
- Sécurité dans les systèmes RAG

Objectifs

- Comprendre l'architecture RAG et ses implications en matière de sécurité.
- Mettre en œuvre les meilleures pratiques pour ancrer et sécuriser les sources de données dans les systèmes RAG.

Activités

- Lab : Génération Augmentée par Récupération (RAG) multimodale à l'aide de l'API Vertex AI Gemini
- Lab : Introduction à l'appel de fonction avec Gemini