

Course : Vertex AI and Generative AI Security

Official Course: Preparation for Google Cloud Certification Exams

Practical course - 2d - 14h00 - Ref. GVS

Price : 1590 € E.T.

NEW

In this training course, you'll learn how to secure generative AI projects using Vertex AI on Google Cloud by protecting data, managing access, securing models and deployments, and applying best practices for oversight and security in applications based on large language models.

Intended audience

AI engineers, cloud architects, developers, and cybersecurity professionals who want to secure generative AI projects using Vertex AI.

Prerequisites

Basic knowledge of machine learning, particularly generative AI. Good written English skills.

Practical details

Teaching methods

The training course is conducted in French. Official course materials are provided in digital format and in English. A good understanding of written English is required.

Course schedule

1 Introduction to Vertex AI Security Principles

- Security on Google Cloud.
- Vertex AI Components.
- Security Issues Related to Vertex AI.

Hands-on work

Training and deploying a custom model with Vertex AI.

PARTICIPANTS

AI engineers, cloud architects, developers, and cybersecurity professionals who want to secure generative AI projects using Vertex AI.

PREREQUISITES

Basic knowledge of machine learning, particularly generative AI. Good written English skills.

TRAINER QUALIFICATIONS

The experts who lead the training courses are specialists in the subjects covered. They are approved by the publisher and certified for the course. They have also been validated by our teaching teams in terms of both professional knowledge and teaching skills for each course they teach. They have at least three to ten years of experience in their field and hold or have held positions of responsibility in companies.

ASSESSMENT TERMS

Assessment of targeted skills prior to training.

Assessment by the participant, at the end of the training course, of the skills acquired during the training course.

Validation by the trainer of the participant's learning outcomes, specifying the tools used: multiple-choice questions, role-playing exercises, etc.

At the end of each training course, ITTCERT provides participants with a course evaluation questionnaire, which is then analysed by our teaching teams. Participants also complete an official evaluation of the publisher.

An attendance sheet for each half-day of attendance is provided at the end of the training course, along with a certificate of completion if the participant has attended the entire session.

2 Identity and Access Management (IAM) in Vertex AI

- Introduction to IAM on Google Cloud.
- Access control via IAM.
- Organizational hierarchies and policies.
- Service accounts and the principle of least privilege.

Hands-on work

Basics of Service Accounts and Roles.

3 Data Security and Privacy

- Data encryption.
- Protection of Sensitive Data.
- VPC Service Controls.
- Disaster Recovery Planning.

Hands-on work

Getting Started with Cloud KMS. Creating a copy of anonymized data in Cloud Storage.

4 Securing Vertex AI endpoints and model deployments

- Network security.
- Securing model endpoints.
- Deploying ML models via endpoints.

Hands-on work

Configuring Private Google Access and Cloud NAT.

5 Monitoring and Logging in Vertex AI

- Event logging.
- Monitoring and metrics.
- Setting up monitoring and alerts.

6 Security Risks in Generative AI Applications

- Threats specific to generative AI applications.
- AI Security and Safety Concepts.
- Prompt Security.
- Protections for LLMs.

Hands-on work

Securing with the Vertex AI Gemini API. Security for LLMs and generative AI for developers.

TEACHING AIDS AND TECHNICAL RESOURCES

The teaching resources used are the publisher's official materials and practical exercises.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training course.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you have specific accessibility requirements? Contact Ms FOSSE, disability advisor, at the following address: psh-accueil@orsys.fr so that we can assess your request and its feasibility.

7 Testing and Evaluating Responses from Generative AI Models

- Testing the generated responses.
- Evaluation and Improvement of Responses.
- Fine-tuning of LLMs.

Hands-on work

Performance Measurement with the Gen AI Evaluation Service. Unit Testing of Generative AI Applications.

8 Securing RAG (Retrieval-Augmented Generation) Systems

- Fundamental Principles of RAG.
- Security Challenges in RAG Architectures.
- Protection of data sources and validation of responses.

Hands-on work

Multimodal RAG with the Vertex AI Gemini API. Introduction to function calling with Gemini.

This programme is an original creation, developed by the teaching teams at ORSYS Formation. Any reproduction, representation, adaptation or use, in whole or in part, without the prior written authorisation of ORSYS, is strictly prohibited. ORSYS reserves the right to take any action necessary to protect its intellectual property rights.

Dates and locations

REMOTE CLASS

2026 : 7 Dec.

2027 : 11 Mar., 24 May, 2 Sep., 22 Nov.

PARIS LA DÉFENSE

2027 : 11 Mar., 24 May, 2 Sep., 22 Nov.