AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 05/06/2024

Sign up

# GuardRails AI training

1 day (7 hours)

## Presentation

Develop AI applications with peace of mind by protecting yourself from inherent risks such as hallucinations, biases, data leaks and toxic language. Our Guardrails AI training course will help you avoid these dangers thanks to the largest library of custom validators.

We'll teach you all you need to know about integrating Guardrails AI into your systems, using validators and guards, as well as the advantages and limitations of the tool.

This tool is open-source and free, so we'll teach you how to install and configure it in the best possible way. By the end of the course, you'll have mastered the GuardRails API syntax and be able to deploy multiple guardrails in a single guard.

Sign up for one of our sessions to become an expert in secure and ethical AI development. We'll be using the latest version, Guardrails AI 0.4.

## Objectives

- Understanding the dangers of artificial intelligence
- Learn how to use validators to secure AI applications
- Installing and configuring Guardrails
- Master the syntax and use of the Guardrails API

## Target audience

- Data Scientist
- Big Data Engineer
- Machine Learning Engineer

- Lead Developer
- Developers
- AI Engineers

## Prerequisites

- Mastery of Python
- Experience using LLM via API

## Guardrails AI training program

### The dangers of artificial intelligence

- Hallucinations
- Safety
- Inappropriate language

### Introducing Guardrails

- Using validators for your AI applications
- Guardrails Open Source vs Guardrails Hub
- List of validators
- What is a Guard?
- Guardrails' limits

### Installation and configuration

- Guardrails installation
- Create a guard
- Launch several guardrails in one guard
- Generate structured data from LLMs

### Guardrails API

- The syntax
- Class
- The arguments
- Using Guardrails with RAIL
- Troubleshooting

## Companies concerned

This course is aimed at both individuals and companies, large or small,

wishing to train its teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

## Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

## Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

## Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

## Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

## Sanction

A certificate will be issued to each trainee who completes the course.