AI Training: Security in AI Projects

Securing AI Agent

Artificial intelligence and language models are revolutionizing our digital world. But they also offer new areas of attack. We read in the media about chatbots whose security mechanisms have been circumvented and about AI being used for attacks. So if AI is to be used effectively and safely, we need to be aware of these dangers and possible security measures.

In this interactive AI security training course, you will learn in a practical way how modern AI systems are vulnerable to attack and, above all, how they can be effectively secured against such attacks. Using many examples and exercises, you will analyze vulnerabilities, carry out attacks yourself and learn how to develop countermeasures and which project architectures are particularly robust against attacks.

Course Contents

- OWASP Top 10 for LLM and Gen AI
- Prompt Injection – Manipulation through Language
- Task Security
- Data Poisoning
- Denial-of-Service Attacks
- Supply Chain Attacks in the AI Ecosystem
- Proper Project Architecture – Excessive Agency as a Vulnerability
- Avoiding Blind Trust – Incorporating Checkpoints

Target Group

This AI training course is aimed at AI managers, Red Team members, safety officers and anyone who wants to use LLMs safely and understand the risks.

Prerequisites

Basic knowledge of AI is an advantage. This can be acquired in the following courses:

Using AI tools and LLMs successfully - ChatGPT, Gemini, Claude & Co. (use of LLMs)

AI manager - potentials, use cases, project know-how (planning AI projects)

Course Target

You will gain the ability to recognize vulnerabilities and attack points of LLMs and understand attacks such as prompt injection. You will be able to develop and implement correct architectures and security concepts for AI projects.

This Course in the Web

You can find the up-to-date information and options for ordering under the following link: www.experteach-training.com/go/**HACL**

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in an non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training		Prices, excl. of V.A.T.
Classes in Germany	**2 Days**	**€ 1,995**
Online Training	**2 Days**	**€ 1,995**

Date/course venue — Course language German

11/05-12/05/26	Frankfurt	03/09-04/09/26	Online
11/05-12/05/26	Online	11/11-12/11/26	Düsseldorf
03/09-04/09/26	Hamburg	11/11-12/11/26	Online

Status 02/10/2026

AI Training: Security in AI Projects

ExperTeach

Our Training Offer for You:

Classroom Training
The live training experience in our training centers or on your premises on-site.

Online Training
Attend your course in online mode – without travel and accommodation expenses and effort.

Hybrid Training
Classroom & online in one course – choose how you wish to participate in your training event.

In-house Training
We create your customized training concepts for your project.

Guaranteed Course Dates
ExperTeach guaranteed course dates allow for secure and reliable planning.

Awards Won by ExperTeach

ExperTeach Benelux B.V.
Ceresstraat 1· 4811 CA Breda· Phone: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach-training.com