

**TRAINING BROCHURE**

# **Responsible AI in software development**



[Provisional reservation >](#)

[Book now >](#)



## Responsible AI in software development

**Price:** € 800 excl. VAT \*

**Duration:** 1 day (remote)

**Contact:** [training@hightechinstitute.nl](mailto:training@hightechinstitute.nl), +31 85 401 3600

### Intro

Generative AI is inevitably transforming the software industry. Tools like ChatGPT or Github Copilot enable developers to code more efficiently than ever before. While this sparks excitement, it also raises concerns, and so many stakeholders tend to balance this optimism with caution. Though these tools are advancing rapidly, to date they still lack the necessary sophistication to consider various subtle but important aspects of software products. This training course emphasizes the importance of understanding this evolution through the well-established principles of responsible AI.

After a short overview of AI and specifically responsible AI, participants delve into the complex world of machine learning (ML), focusing on how these solutions can be compromised. Threats and vulnerabilities such as model evasion, poisoning and inversion attacks are explained in a simple way, via real-world case studies and live demonstrations. Finally, we overview the security challenges of large language models (LLMs), exploring the practical defenses as well.

The course then highlights the capabilities and limitations of generative AI (GenAI) tools - like Github Copilot, Codeium or others -, offering insights into their role in code generation and beyond. Topics include smart prompt engineering, not only during the implementation phase but also during requirements capturing, design, testing and maintenance. Participants will learn best practices and pitfalls of using AI-generated code, with hands-on labs demonstrating potential security flaws such as dependency hallucination and path traversal. By the end, software engineers and managers will have a clear understanding of how to responsibly integrate GenAI tools into the various stages of the software development lifecycle.

### Objective

- Understand various aspects of responsible AI
- Essentials of machine learning security
- How to use generative AI responsibly in software development
- Prompt engineering for optimal outcomes
- How to apply generative AI throughout the SDLC

### Target audience

All people involved in using GenAI or developing machine learning (developers, testers, managers).



### Certification

Participants will receive a High Tech Institute course certificate for attending this training.

### Trainers

[Balazs Kiss](#)

*\* Prices are subject to change. Price correction will be applied at the end of the year.*

Keep me posted



## Program

### A brief history of artificial intelligence

- The origins of AI
- Neural networks and “probability engines”
- Robustness of ML systems
- Early ML coding tools
- The AI coding revolution of the 2020s

### Responsible AI

- What is responsible AI?
- Accountability and transparency
- Mitigation of harmful bias
- Validity and reliability
- Lab - Experimenting with reproducibility in Copilot
- Explainability and interpretability
- Safety, security, privacy and resilience
- Security and responsible AI in software development

### An overview of AI and ML security

- A quick overview of ML for non-specialists
- GIGO and other well-known ML pitfalls
- Malicious use of AI
- Real-life attacks against AI
- Subverting AI to attack others
- AI and ML security standards
- A quick look at ML hacking: evasion
- A quick look at ML hacking: poisoning
- A quick look at ML hacking: model inversion
- A quick look at ML hacking: model stealing
- The security of large language models

### Using GenAI responsibly in software development

- LLM code generation basics
- Basic building blocks and concepts
- GenAI tools in coding: Copilot, Codeium and others
- Can AI... take care of the ‘boring parts’?
- Can AI... be more thorough?
- Can AI... teach you how to code?
- Lab - Experimenting with an unfamiliar API in Copilot
- GenAI as a productivity boost
- The dark side of GenAI
- Prompt engineering techniques for code generation
- Integrating generative AI into the SDLC
- Security of AI-generated code

### Summary and takeaways

- Responsible AI principles in software development
- Resources and additional guidance

## Methods

Live, instructor-led online classroom training. Discussions. Hands-on practice using case studies and live lab exercises.

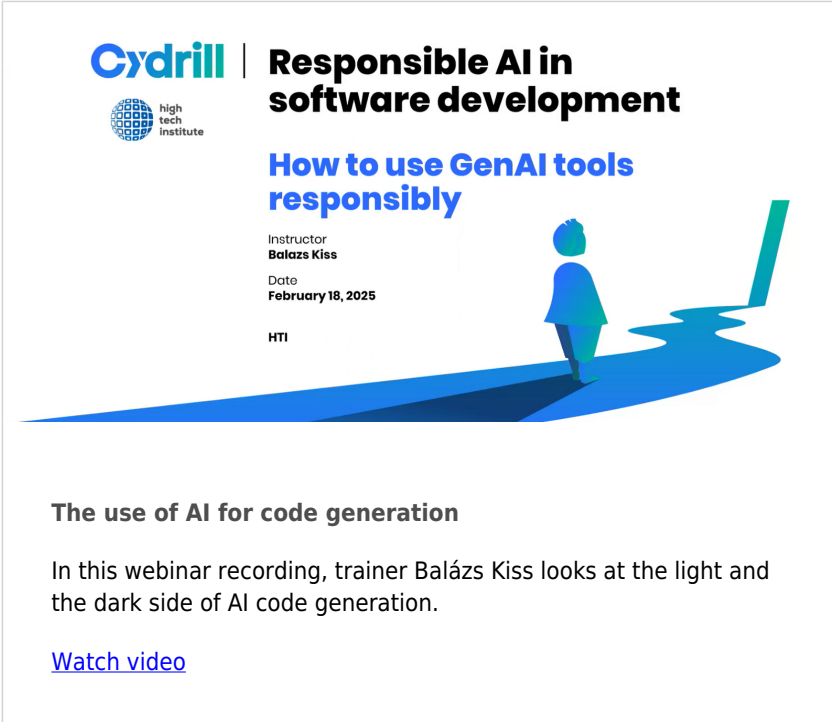
## Trainers

Balazs Kiss

## Frequency

Twice per year

## More information



The image shows a webinar recording cover. At the top left is the Cydrill logo, which includes a globe icon and the text 'high tech institute'. To the right of the logo, the main title reads 'Responsible AI in software development'. Below this, the subtitle is 'How to use GenAI tools responsibly'. The instructor's name, 'Balazs Kiss', and the date, 'February 18, 2025', are listed. The HTI logo is at the bottom left. The central graphic depicts a stylized blue figure standing on a path that leads towards a glowing blue screen, symbolizing the journey into AI.

**Cydrill** | **Responsible AI in software development**

high tech institute

**How to use GenAI tools responsibly**

Instructor  
**Balazs Kiss**

Date  
February 18, 2025

HTI

**The use of AI for code generation**

In this webinar recording, trainer Balázs Kiss looks at the light and the dark side of AI code generation.

[Watch video](#)

Read the interview:



A man with short grey hair and a nose ring, wearing a black t-shirt with a 'code' logo, stands against a blue background. The logo on his shirt features the word 'code' in a stylized font with vertical lines of varying heights below it.

Trainer Balázs Kiss about using AI responsibly

*"With the present state of generative AI, it's possible to write code without understanding programming. However, if you don't understand the generated code, how will you maintain it?"*