Vibe Coding: AI-Powered Coding and Security Principles

Duration: 4 days
Audience: Professionnel TI

Who is this training for?

Developers, IT project managers, AI and cybersecurity teams wishing to integrate Vibe Coding into their software development practices.

Training objectives

- Positioning Vibe Coding in the Software Development Lifecycle (SDLC)
- Understand how Vibe Coding fits into the different phases of the SDLC and helps optimize development processes.
- Write prompts that comply with industry standards
- Learn how to formulate clear, safe and effective instructions to generate code that complies with good safety and quality practices.
- Identify risks related to AI-generated applications
- Be able to identify potential vulnerabilities (dependencies, insufficient documentation, security or licensing issues) and propose solutions to correct them.
- Implement a code review and secure deployment approach
- Use tools, checklists and proven practices to ensure the reliability, compliance and security of deliverables

Summary

This program introduces participants to the practices of AI-assisted development (""Vibe Coding"") while integrating essential security principles. The learning path combines theory, practical examples, and collaborative workshops, to develop a critical understanding of the opportunities and risks of generative AI in software development.

Course outline

Copyright © 2026 AFI by Edgenda inc.

Week 1: Software Development Practice and Vibe Coding

- Overview of SDLC and CI/CD Pipelines (Plan, Coding, Test, Deploy, Maintain).
- Learn how Vibe Coding accelerates rapid prototyping with low-code and AI model integration.
- Risk analysis (lack of version control, hidden dependencies, reproducibility issues) and practical comparison: creating a "to-do" application with Vibe Coding vs. classic workflow.

Week 2: Safe prompt writing practices

- Principles of prompt engineering applied to security: accuracy, constraints, test cases.
- Examples of safe and unsafe prompts.
- Introduction to Security Frameworks (OWASP Top 10, Least Privilege).
- Convenient: Improving imperfect prompts to secure versions.

Week 3: Vibe Coding Application Security Pitfalls

- Learn how to use Copilot to transform your conversations in Teams, your emails in Outlook, and your project follow-ups.
- Automate tasks, gain clarity, and improve coordination across your teams.

Week 4: Code review and secure deployment

- Principles of security code review adapted to Vibe Coding: checklist (authentication, authorization, data validation, error handling, logging).
- Deployment considerations (API keys, secrets management, environment configuration).
- Practical: cross-review, application of the checklist and securing the code.
- Conclusion on best practices and resources for the safe use of Vibe Coding.

Approach and methodology

The training favours a hybrid and experiential approach, combining theoretical capsules, concrete demonstrations and collaborative practical workshops, to anchor learning in real development situations. Participants are asked to compare, experiment and improve (e.g. prompts, generated code, security practices) through concrete cases and cross-reviews. The progressive course over 4

Copyright © 2026 AFI by Edgenda inc.

weeks promotes a continuous increase in skills, integrating critical reflection, practice and structured feedback.

Recommendations

We recommend that learners have beforehand:

- Basics in software development or equivalent content
- Notions of artificial intelligence or equivalent content
- Computer security awareness or equivalent content

Copyright © 2026 AFI by Edgenda inc.