What AI-generated code gets wrong

(and how to catch it)

AI-generated code often contains hidden risks such as outdated security patterns, predictable logic, and missing validations. Because AI trains on public (often insecure) code, vulnerabilities can sneak into your project unnoticed. SonarQube acts as an independent verification platform by objectively scanning every line of code for leaks and bugs.

With strict quality gates, it blocks insecure generated code before it reaches production. This way, you combine the speed of AI with the confidence of security control.

AI-specific quality gates

You can set stricter rules for code generated by AI. Where a human developer might get away with 80% test coverage, you can require 100% from generated code before it passes through the pipeline.

Deep analysis and taint analysis

SonarQube looks beyond the surface. It detects complex security vulnerabilities (such as insecure data streams) that remain hidden from the AI-generated text by the human eye or a simple linter.

Hardcoded secret detection

AI tends to insert temporary passwords or API keys into code. SonarQube recognizes more than 450+ "secret patterns" and immediately blocks the code if they are present.

AI CodeFix and remediation

Using Sonar AI CodeFix, developers can receive a tailored fix suggestion generated by LLMs that are context aware of the entire codebase, ensuring the suggested solution isn't just generic code substitution. . Whether the code is written by a senior developer, a junior, or an AI agent, SonarQube applies the same objective yardstick to everyone. This prevents poor quality code from slowly polluting your project.

Responsible agent-centric development

The pace of AI-assisted development is transforming how DEPT builds software, which also introduces new security challenges. With SonarQube, they can move fast without compromising on quality, security, or compliance. It delivers the automated code checks and safeguards needed to stay innovative and confident, even with AI generated code.

Innovation should never come at the cost of quality. One of our prime partners is supporting clients with the implementation of SonarQube to enhance code quality. Wesley Niels (Director Cloud) from DEPT® says: "We didn't partner with Sonar just to improve code, we did it to redefine how we build software. By using AI CodeFix and adopting the Agent Centric Development Cycle, we embed verification, security, and quality into every step of the development process. This allows us to move faster without losing control, delivering stronger products and better outcomes for our clients."

SonarQube helps ensure that speed never comes at the cost of trust. Teams are empowered to innovate freely while maintaining full control and confidence in every line of code.