AI CODING ASSISTANTS

IN FOCUS: GitHub Copilot, a language-agnostic coding tool that makes real-time suggestions inside the developer's coding environment.

Beyond the hype and hysteria, AI-powered coding assistants show real potential to support enterprise software development. To get the most out of these tools, you need to understand risks and mitigations.

> Your AI Coding Assistant Has Potential Issues You Need to Be Aware of.

It Has Issues With Predictability, Reliability, and Consistency.

Change one small word, e.g., type

Remove all items instead of **Delete** all items

...and you can get different results.

Repeat an error in your code, and you risk getting repeated errors in recommendations.



There Are No Secure Defaults

The default code suggestions may be vulnerable. The suggested libraries may be insecure, out-of-date, deprecated, or unsupported.



It Lacks Contextual Knowledge of Application Architecture (and can't see the forest for the trees)

knowledge needed to provide more applicable suggestions. So, if you're working on a larger architecture, it won't get the bigger picture and adjust suggestions accordingly.

The tools lack the contextual



(but if it gets it wrong, you won't know)

You Depend on It When Navigating Unfamiliar Territory

territory e.g., new programming language, but when it gets something wrong, the developer may not catch it due to their lack of familiarity with the language.

It may help you navigate unfamiliar



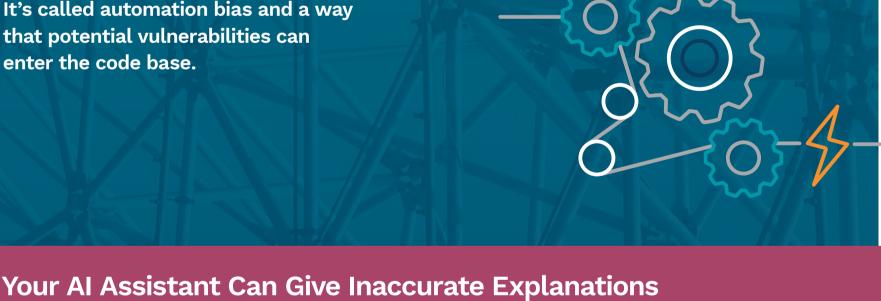
from Your Automated Copilot

...And You End Up Always Trusting the Default Suggestions

enter the code base.

It's called automation bias and a way

that potential vulnerabilities can



Just like a human, the tool can incorrectly

documentation will be inaccurate.

incorrectly. Meaning your explanations or

analyze code or summarize changes

It's Delivered as-a Service

collected, stored, or used. AI coding



You have no control over how your data is

Which Could Lead to Data Leakage and Privacy Issues

- Microsoft/GitHub, OpenAI, etc. They decide what data they use or share, which can lead to issues with loss of sensitive data and intellectual property.

assistants are hosted on third-party sites



Mitigating Risks Although automated coding

Strategy For

assistants are relatively new, many existing tools and processes can address these new risks.

Discovery Awareness

Process

Tooling and Testing

Specificity

Read the report to find out more



info@kudelskisecurity.com | www.kudelskisecurity.com