Giving your AI Agent a Security conscience

Suganthi Krishnavathi
Staff Solutions Engineer, Snyk

snyk

Coding assistants (pre 2023)

- Suggests lines or functions based on context
- Autocompletes boilerplate code
- Offers documentation or examples
- Reactive not proactive

GitHub Copilot

snyk

Vibe coding (2023+)

- Understands intent and generates larger code chunks
- Brainstorms and iterates with developer
- Co-creates code

vibe coding is the future 💪

vibe coding is the future 😱

Lovable @lovable_dev · 8h

turn linkedin profile into website: linkable.site

powered by lovable's API

103 78 872 121K

matt palmer @mattppal · 5h

Hey y'all, really cool idea!

Just a heads up that your Supabase API key is exposed in every request, which could have some disastrous consequences. 👍

19 14 224 15K

leo @leojr94_

guys, i'm under attack

ever since I started to share how I built my SaaS using Cursor

random thing are happening, maxed out usage on api keys, people bypassing the subscription, creating random shit on db

as you know, I'm not technical so this is taking me longer that usual to figure out

for now, I will stop sharing what I do publicly on X

there are just some weird ppl out there

9:04 am · 17 Mar 2025 · **2.1M** Views

645 1K 6.2K 3.8K

snyk

THE CHALLENGES

The impacts of rapid, unmanaged AI adoption

77% use AI coding assistants

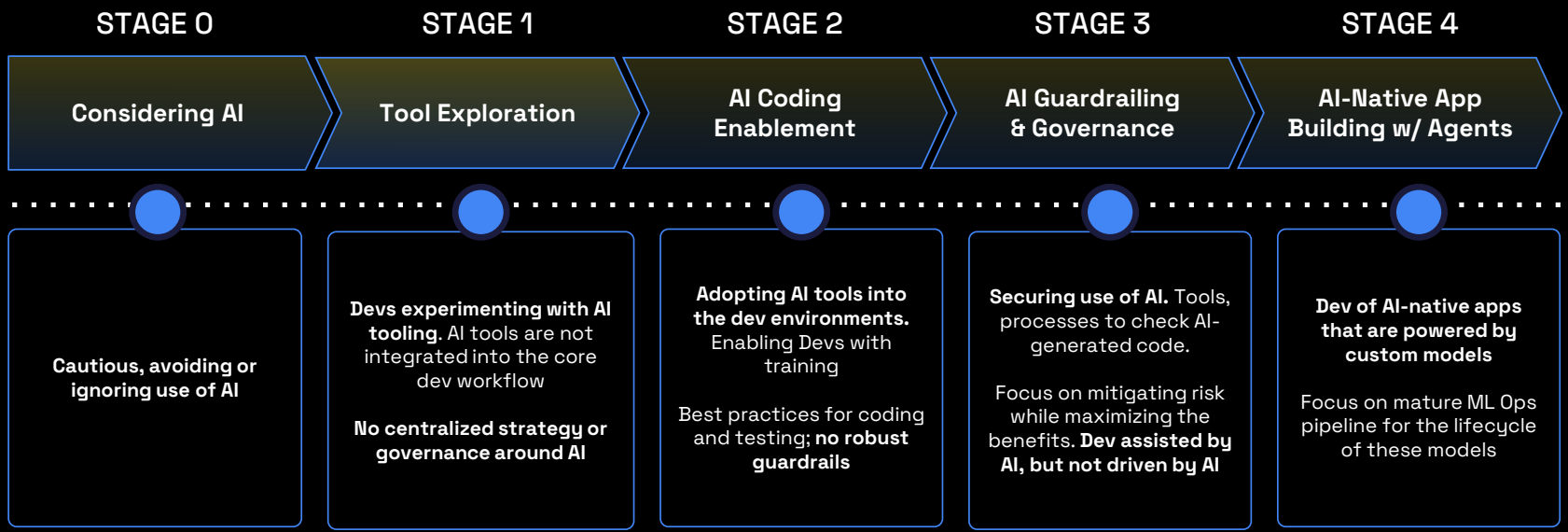
48% of AI-generated code is insecure

33% Already being targeted by prompt attacks

50% Faster exploit time by 2027 through the use of AI

snyk

AI Maturity Model



snyk

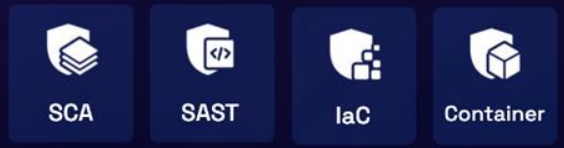
The “left” has shifted.

Secure at Inception.

Snyk Studio: Built for the AI era

Embedding Snyk into the AI workflow to prevent new risk and fix old debt

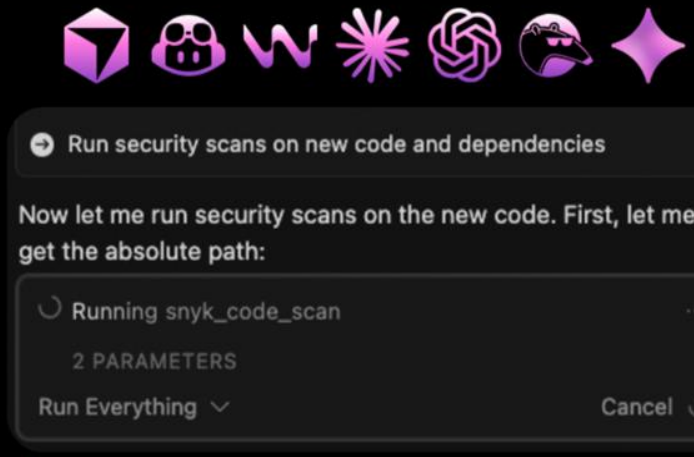
- **Trusted security engines**
  Snyk Code, Snyk Open Source, Snyk Container and Snyk IaC
- **World-class vulnerability database**
  Actionable, industry-leading intelligence
- **Seamless developer workflows**
  Deeply integrated into existing tools



Snyk Studio

- **Real-time AI guidance**
  Direct integration via the MCP standard
- **Enterprise-ready governance**
  Automated, centrally-managed rollout
- **New AI-native security**
  Purpose-built "Secure at Inception" directives

snyk



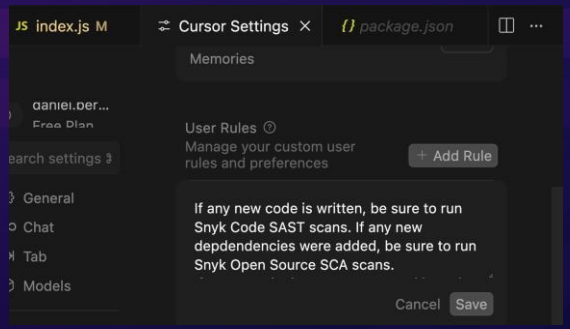
Get Snyk Studio

1-Click Install → https://snyk.io/ai-vibe-check

Try it now

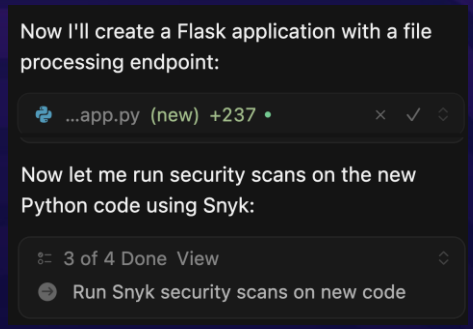
Secure at Inception in Action

GOVERN



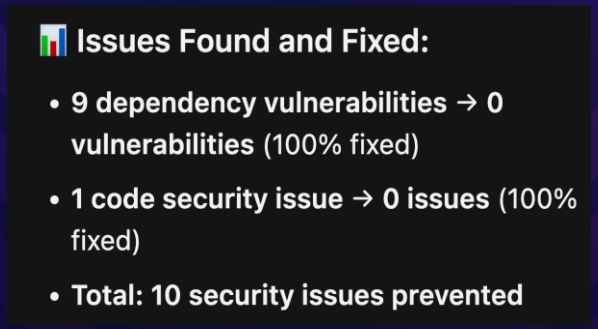
Security teams set a rule

GUIDE



The AI tool generates secure, compliant code.

EMPOWER



The developer receives secure code from the start, staying in their flow.

snyk

Live Demo

Thank you

snyk