USE CASE

Pass the enterprise security questionnaire with evidence

Aribot scans your repositories and pipelines and turns the fixes into the SOC 2 evidence an enterprise buyer's questionnaire asks for.

THE PROBLEM

A Series B company sells to enterprises, and every deal brings a security questionnaire. The answers live in people's heads, the evidence is screenshots, and the security lead spends weeks per quarter on paperwork instead of security.

HOW ARIBOT HANDLES IT

1. **Scan repos and pipelines**
   Find code flaws, secrets, risky dependencies and pipeline misconfigurations.
2. **List APIs and AI calls**
   Answer what your product exposes and which AI models it calls.
3. **Map to SOC 2 and ISO 27001**
   Each fix becomes evidence against the controls the questionnaire asks about.
4. **Run it on every build**
   Call Aribot from CI so the evidence stays current.

WHAT YOU SEE IN THE DEMO

- Code Review: findings tied to lines
- Compliance Standards: controls and the frameworks they serve
- Agent Assurance: what your AI features can reach

WHO IT IS FOR

Head of Security · DevSecOps Lead · VP Engineering · CTO

WHAT YOU GET

- Questionnaire answers backed by records
- SOC 2 and ISO 27001 evidence from normal engineering work
- An inventory of APIs and AI calls for the AI questions buyers now ask
- Pay per scan, no seat licence

40%

of enterprise apps are expected to feature task-specific AI agents by 2026 (Gartner says up to), from under 5% in 2025

Source: Gartner press release, 26 Aug 2025

See it: ayurak.com/demos/code-review

€50 per review · €40 per pipeline scan · €75 per compliance scan