
USE CASE

Code findings tied to the line that caused them

Paste code and get findings mapped to STRIDE and MITRE ATT&CK, each tied to the line that produced it and paired with a recommended fix.

THE PROBLEM

Our security review is a gate at the end of the sprint, and developers wait on it.

Too many of the alerts are noise, so developers have stopped trusting them. When a real finding lands, nobody can see which line caused it or what to change.

WHY IT MATTERS NOW

59%

worry that AI coding tools will introduce vulnerabilities into their code

Source: Snyk State of Open Source Security 2023

HOW ARIBOT HANDLES IT

1 **Paste the code**

Drop in a snippet, such as an API endpoint.

2 **Analyse it**

Aribot raises threats by STRIDE category and marks the line each one comes from.

3 **Map to MITRE ATT&CK**

Findings are mapped to ATT&CK techniques and tactics.

4 **Get the fixes**

Each recommendation comes with a priority, an effort estimate and a code example.

WHAT YOU GET

- Findings tied to specific lines of code
- STRIDE category and MITRE ATT&CK technique on each finding
- Recommended fixes with code a developer can check
- The same analysis available through the API for your build pipeline

SEE IT IN THE DEMO

- A sample checkout endpoint with the flagged lines highlighted
- Tabs for threats detected, MITRE ATT&CK mappings and fixes
- Findings such as missing authentication, missing input validation and no rate limiting, each with its impact
- Fix cards with priority, estimated effort and a code snippet

See it for yourself

ayurak.com/demos/code-review

€50 per review · €40 per pipeline scan · €25 per SBOM