
USE CASE

Turn a plain-language brief into a threat-modelled design

Describe the system you want in plain language, and Aribot turns it into a cloud architecture and a threat model that stay linked to the live estate.

THE PROBLEM

Leadership describes a new platform in a few sentences, and the architects spend weeks turning that into diagrams.

Security review comes last, after the big decisions are made. Once the system is live, nobody checks that what runs still matches what was designed.

WHY IT MATTERS NOW

95%

of security teams report a skills gap; 59% call it critical or significant

Source: ISC2 Workforce Study 2025

HOW ARIBOT HANDLES IT

1 **Describe the system**

Write what you need in plain language, for example a payment tracking API on a named cloud provider.

2 **Generate the architecture**

Aribot proposes a cloud architecture with real services, data flows and network boundaries.

3 **Model the threats**

Each component is analysed and mapped to STRIDE and MITRE ATT&CK, with every finding tied to its component.

4 **Connect the live estate**

Read-only cloud accounts are mapped back to the diagram, so drift shows up against the design.

WHAT YOU GET

- A first architecture and threat model from a written brief
- Threats tied to named components, each open to review
- A design that stays linked to the cloud resources that implement it
- A shared starting point for architects and leadership

SEE IT IN THE DEMO

- Phases that run from executive intent and a plain-language brief through architecture, threat modelling, code security, infrastructure as code and live monitoring
- Example briefs a CTO or CIO might write, such as moving a core banking ledger to cloud-native services
- A generated architecture with gateway, compute, database, messaging and key management services
- Per-component threat examples mapped to STRIDE and MITRE ATT&CK techniques

See it for yourself

ayurak.com/demos/vision-to-ops

€600 per diagram, three regenerations included · free
Starter tier with one diagram