

USE CASE

Threats per component, straight from your architecture

Aribot reads your architecture and attaches threats to each component, mapped to STRIDE and MITRE ATT&CK, so design review keeps up with delivery.

THE PROBLEM

Threat modelling is the first thing we skip when delivery is under pressure. The models we do write go stale within a quarter. Leadership never sees which new systems were modelled before launch.

HOW ARIBOT HANDLES IT

- 1 **Load the architecture**
Start from a diagram of your services, gateways and data stores.
- 2 **Run the analysis**
Aribot walks the components and connections and raises threats as it goes.
- 3 **Read threats per component**
Each threat sits on the component it affects, such as spoofing on an auth service or tampering on a database.
- 4 **Check the mapping**
Threats are labelled against STRIDE, PASTA and MITRE ATT&CK.

WHAT YOU SEE IN THE DEMO

- An infrastructure topology with a client, a gateway, services and databases
- Threats appearing on each node as the analysis runs
- A Threats Detected list covering STRIDE categories such as spoofing, tampering, repudiation and denial of service
- Hover detail on each flagged node

WHO IT IS FOR

- Security Architect
- Threat Modelling Lead
- Head of Security Architecture
- CISO

WHAT YOU GET

- A threat model for every new system, built from its diagram
- Threats attached to named components
- STRIDE and MITRE ATT&CK mapping on each threat
- A starting point for attack paths, security requirements and controls

52%

have no regular management reporting on threat modelling

Source: Threat Modeling Connect, State of Threat Modeling 2024-25

NIS2 · 17 Oct 2024

Operators in essential sectors need documented design reviews and a control map for new systems.

DORA (EU financial sector) · 17 Jan 2025

ICT risk management covers new and changed systems, and each one needs a threat model on file.

See it: ayurak.com/demos/threat-modeling

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