USE CASE

Plant and cloud attack paths, mapped to NIS2

Aribot models your plant and cloud architecture, shows the attack paths that matter and maps the controls to NIS2, so management can show it is in control.

THE PROBLEM

NIS2 makes management personally accountable for cyber risk. Plants connect operational technology to the cloud, little software is written in-house, and the board wants to know which risks are real.

HOW ARIBOT HANDLES IT

1. **Model the connected plant**
   Draw or upload the plant and cloud architecture.
2. **Simulate the attack paths**
   Map techniques to MITRE ATT&CK and see which components they reach.
3. **Map controls to NIS2**
   Each control shows the NIS2 obligations it supports.
4. **Report to the board**
   Show exposure in currency, with what is measured and what is not.

WHAT YOU SEE IN THE DEMO

- Threat Modeling: threats per component
- Attack Simulation: paths mapped to ATT&CK
- CXO Workbench: exposure in currency with coverage

WHO IT IS FOR

Head of IT Security · OT Security Manager · CIO · CISO

WHAT YOU GET

- Attack paths across plant and cloud
- A NIS2 control map tied to the architecture
- A board view of exposure with its coverage shown
- Threat models that stay current with the cloud

NIS2 · 17 Oct 2024
The transposition deadline has passed and national laws are landing; enforcement is tightening.

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

€600 per diagram · €150 per war-game / path-to-green · €75 per compliance scan