A GLOBAL AGRIFOOD MANUFACTURER

From a request form to a signed-off threat model

The security governance team wanted every new system to get a threat model without the team becoming the bottleneck. Aribot now takes the request, works out which frameworks apply from the answers, opens the work in ServiceNow and tracks it to sign-off.

8

frameworks the intake can scope automatically, including ISO 27001, ISO/IEC 42001, SOC 2 and NIST CSF 2.0

15 min

between ServiceNow and Aribot ticket reconciliations, on top of instant webhooks

20 of 20

answers matched when an exported Microsoft Forms response was imported in acceptance testing

THE SITUATION

Project teams were already asking for security reviews through a Microsoft Form, and the governance team already worked from ServiceNow. Neither was going to change.

The team set three requirements. The same answers must always lead to the same frameworks, whoever reads the request. The threat model and its ticket must never disagree for long. And every review needs a named owner, a due date and a sign-off.

WHAT WE BUILT

An intake that asks the right questions

The intake questionnaire covers eight governance areas, from data handled to use of AI. Teams that already filled in the Microsoft Form do not start again: their export imports straight in.

Scoping from the answers, not from memory

Each answer sets a signal, such as personal data in scope, AI in use or financial data handled. The signals decide which frameworks apply. 'No' and 'Unknown' do not trigger a framework, so scope only grows when the facts say it should.

ServiceNow stays in step

Aribot opens the ticket and both systems keep each other current. ServiceNow pushes changes through a signed webhook, and a reconciliation every fifteen minutes catches anything a webhook missed.

Ownership and sign-off

Each threat model has an owner and a due date, and reminders go out before it is late. Findings can be assigned to individuals. A model moves through review to sign-off, and approved design patterns can be reused on the next system instead of being argued again.

RESULTS

- The same answers always produce the same scope. Scoping no longer depends on who picks up the request.
- A finished review and its ServiceNow ticket cannot disagree for longer than one fifteen-minute reconciliation.
- Responses already collected in Microsoft Forms import without retyping.
- Usage figures are deliberately left out until the programme has run a full quarter.

NEXT

Planned next: sign-in through the company's own identity provider, so project teams request reviews with the account they already use.

RELATED USE CASES

Threats per component, straight from your architecture · Architecture, threats, controls and cloud evidence on one canvas · Framework scores that show how many controls were assessed

Customer name withheld. This study describes what was built and how it works. Usage figures will be added after a full quarter of live requests.

Products: AI Threat Modeling & Unified Workbench, Compliance Scan & Ayurak Trust