

Project Tuttwiler — Tier■1 Triage MVP

Executive Summary

Problem

Under■resourced operators in the bioeconomy (small hospitals, labs, food/agriprocessors) are flooded with cyber/bio advisories and cannot tell what applies to them, how to prioritize, or what to do.

Target User

The overworked technical lead at a small but critical operation (e.g., rural hospital IT admin, diagnostics lab manager, food safety supervisor) without a 24/7 SOC who receives many alerts.

What “Good” Looks Like

A mission■control triage assistant that ingests signals, de■dupes, validates provenance, ranks by human impact (not just CVSS), and presents one decisive card with the right next step.

Our Approach (7 Features)

- Mission Control View — one priority card at a time; GO / HOLD / ESCALATE.
- Human Impact Index — scores direct care risk, accuracy, exploitability, patch status, dependency.
- Safe Action Playbooks — short, regulated■environment■safe steps (no one■click shutdowns).
- Source Provenance — receipt of origin, TLP, confidence; defend against spoof/poisoning.
- “Is This Us?” Filter — local relevance question to suppress non■applicable noise.
- Tier■2 Escalation — one■click package to Bio■ISAC with context and audit trail.
- Quiet Mode — only human■safety (RED) alerts break through during protected windows.

Architecture at a Glance

Ingest (CVE/CISA/vendor/OEM/news) → Normalize/Dedupe/Provenance → AI summarize + propose score → Human triage (GO/HOLD/ESCALATE) → Action/Notify -

Value

Fewer, smarter alerts; safer first steps for small teams; auditability and trust. Focus shifts from “read endless advisories” to “do the right next thing.”

Next Phase (SOW)

- Automate intake from trusted feeds; expand allowlist/denylist and confidence scoring.
- Lightweight user verification to protect sensitive guidance; role■aware access.
- Logging & audit export; Tier■2 workflow and override governance.
- Pilot Quiet Mode policy and Human Impact Index tuning with one real site.