Architecture & Data Flow — Tier■1 Triage

Ingest → Normalize/Dedupe → AI Assist (Summarize/Score) → Human Triage → Action/Escalate → Audit

Ingest & Normalize

CVE/NVD

CISA/CERT

Vendor Bulletins

OEM Notices

Sector Newsletters

Ransomware Feeds

Validate, Dedupe, Provenance

• Hash/URL dedupe • Source allowlist/denylist • TLP tag • Confidence score

• Poisoning/spoof checks (domain/verbatim match) • Unverified → queue for Tier■2 validation

AI Assist + Human-in-the-Loop Triage

AI: Summarize advisories; propose priority via Human Impact Index.

Human: Confirm relevance (“Is this us?”), adjust score, choose GO / HOLD / ESCALATE.

GO

HOLD

ESCALATE

Actioning & Escalation

• Apply Safe Action Playbook • Quiet Mode policy • Notify stakeholders

• Escalate to Bio■ISAC Tier■2 with context • Create audit/event log

Future Phase: automate ingest; add lightweight verification; export audit to SIEM; integrate asset inventory where available.