Data Sources — Allowlist & Validation

Signals we consider, and how we trust them

Primary Allowlist (trusted by default)

- CVE/NVD (NIST) — canonical CVE feed; use CVSS with caution; capture CVE IDs.
- CISA/CERT advisories — sector alerts, ICS/medical bulletins.
- Vendor & OEM security portals — advisories, patches, mitigations (Siemens, GE, Abbott, etc.).
- National/International CERTs — US■CERT, CERT■EU, ACSC, etc.
- FDA/EMA notices (device/software where applicable).
- Academic/peer■reviewed sources for bio/assay impacts (when present).

Secondary Sources (review + verify)

- Sector newsletters and ISAC partner notes.
- Well■known threat intel blogs and DFIR posts.
- Ransomware/victim leak trackers (signal for active targeting).
- Community reports (GitHub issues, forums) — treat as unverified until replicated.

Denylist / High■Risk (avoid or quarantine)

- Anonymous pastes with no provenance.
- Sites known for spoofed advisories or scam patches.
- Screenshots without original link or cryptographic signature.

Validation Steps (every alert)

- Record provenance: origin URL, timestamp, TLP, hash of content, and author org.
- Cross■check at least two sources for critical claims or 'no■patch' assertions.
- Dedupe by CVE/URL hashes; collapse repeats to reduce fatigue.
- Tag confidence: High (vendor/CISA), Medium (reputable blog + vendor link), Low (community only).
- Escalate unverified claims to Tier■2; do not auto■notify operators.

Data Handling & Ethics

- Respect TLP markings; restrict sharing of TLP:AMBER/RED outside intended audience.
- Remove sensitive indicators from public artifacts; keep in audit store only.
- Attribute sources in internal notes; avoid paywalled content reproduction.