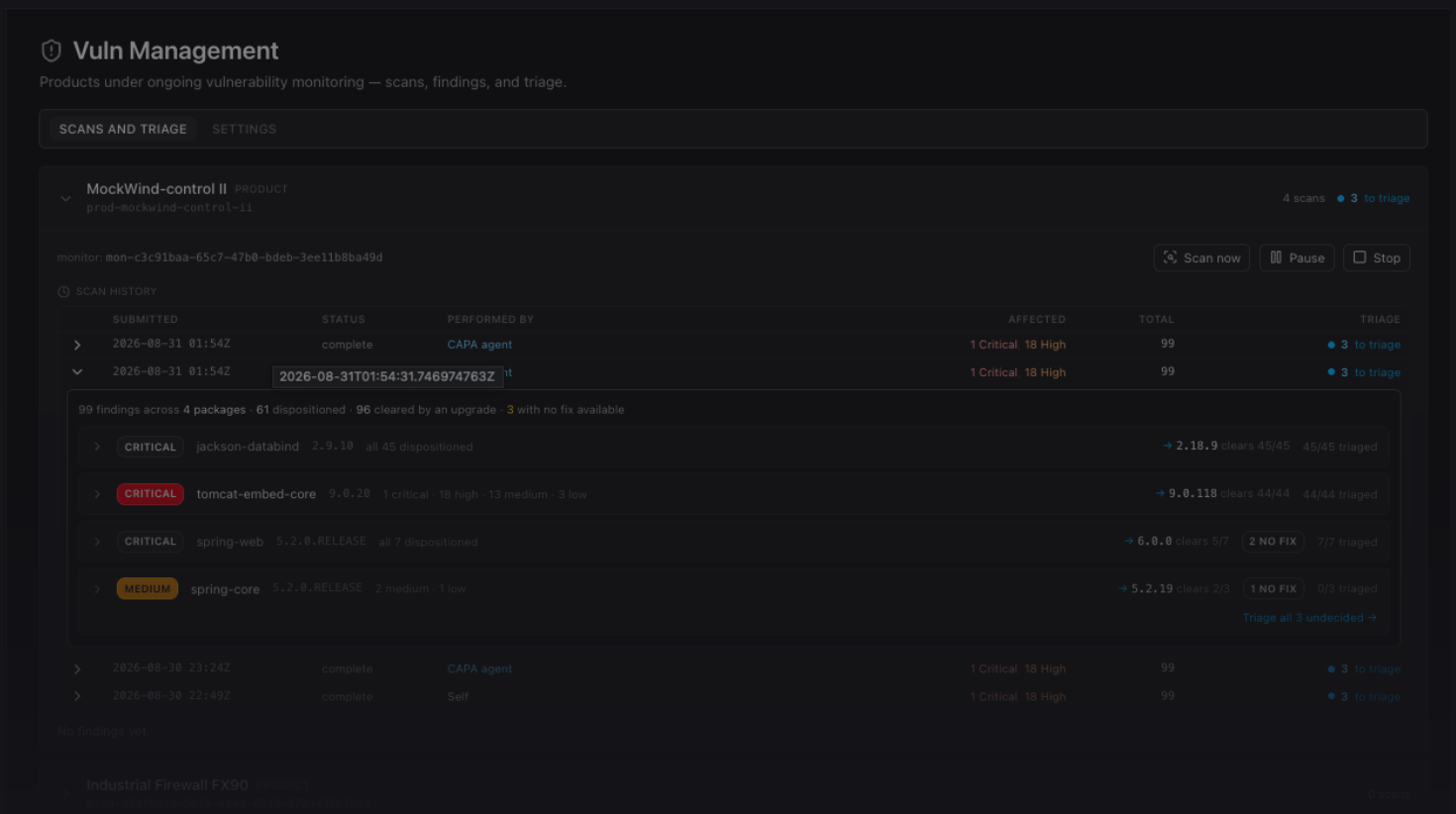



CAPA SECOPS SUITE

# Supply Chain Assurance

## Securing your IT and OT supply chain

Supply chain compromise is one of the most common attack vectors on critical infrastructure. Under Australia's enhanced CIRMP obligations, made under the SOCI Act, operators must map their vendor supply chains, obtain assurance that software is vetted for vulnerabilities and malware, and run tamper-proof patch management across IT and OT environments.

CAPA Aquila delivers a two-sided assurance capability — for OEM product vendors and for renewables operators — providing attestation, trust and authenticity for every digital system installed and operated within IT and OT critical infrastructure. The capability is delivered in three tiers.

CAPA\

THE CHALLENGE

# You carry the risk but lack the visibility.

*A renewable asset is an assembly of a dozen manufacturers across as many jurisdictions. The operator holds the obligation; almost none of the evidence sits inside the operator's control.*

A single wind farm or BESS runs turbine or inverter controllers, a plant controller, SCADA and historian, protection relays, edge network devices, metering and condition monitoring — plus the OEM cloud platforms behind them. Those products are built from thousands of third-party software components, delivered through integrators, and maintained by contractors under long-term service agreements that require standing remote access.

The operator holds the licence, the connection agreement and the regulatory obligation. The vendors hold the knowledge. Under the Australian enhanced CIRMP obligations under SOCI, that gap is now a compliance problem as well as a security one: operators must map the supply chain, obtain assurance that software is vetted for vulnerabilities and malware, and run tamper-proof patch management across IT and OT.

> *The operator is accountable for a supply chain it cannot see, cannot test, and with legacy contractual arrangements*

### The questions that we should be asking:

- What is actually inside the products we run — components, libraries and firmware, and who wrote them?
- How do vendors reach our plant remotely today, from where, and under what conditions are they able to patch software systems?
- When a critical vulnerability is published, who performs triage and how quickly do we know if it is material?
- Can we prove the image running as a supervisory controller is the one the vendor built and released?
- What are the governance structures for each vendor, and has that changed since we procured them?
- If a vendor platform is compromised or withdrawn, can we still operate and recover?

### Where today's practices expose risks to operators:

**Qualitative assurance**

Questionnaires — a compliance driven annual tick-box exercise, self-attested and unverifiable and not managing risk.

**Spreadsheet inventories**

A hand-maintained list of products without sub-components or versions that very quickly goes out of date, with no record of the production state.

**Contractual flow-down**

Clauses oblige the vendor to be secure but with no clear metrics or reporting, and no assurance regime as a result.

**Patch when you can**

OT patching is bounded by warranty, availability and maintenance windows with little to no involvement and oversight by the operator.

THE SOLUTION

# What good assurance looks like

*Six characteristics separate a working assurance capability from a documented intention.*

1. **A live registry, not a spreadsheet**

   Every product, version and sub-component in the estate, held per site and updated as the plant changes rather than as the audit approaches.

2. **Vendor evidence, independently verified**

   SBOMs and signed attestations produced at release and checked on receipt — not a declaration taken at face value once a year.

3. **Vulnerability intelligence tied to your estate**

   PSIRT and VEX feeds monitored across the whole vendor ecosystem, triaged against the products and versions you actually run, and tracked to closure against an SLA.

4. **Chain of custody from build to site**

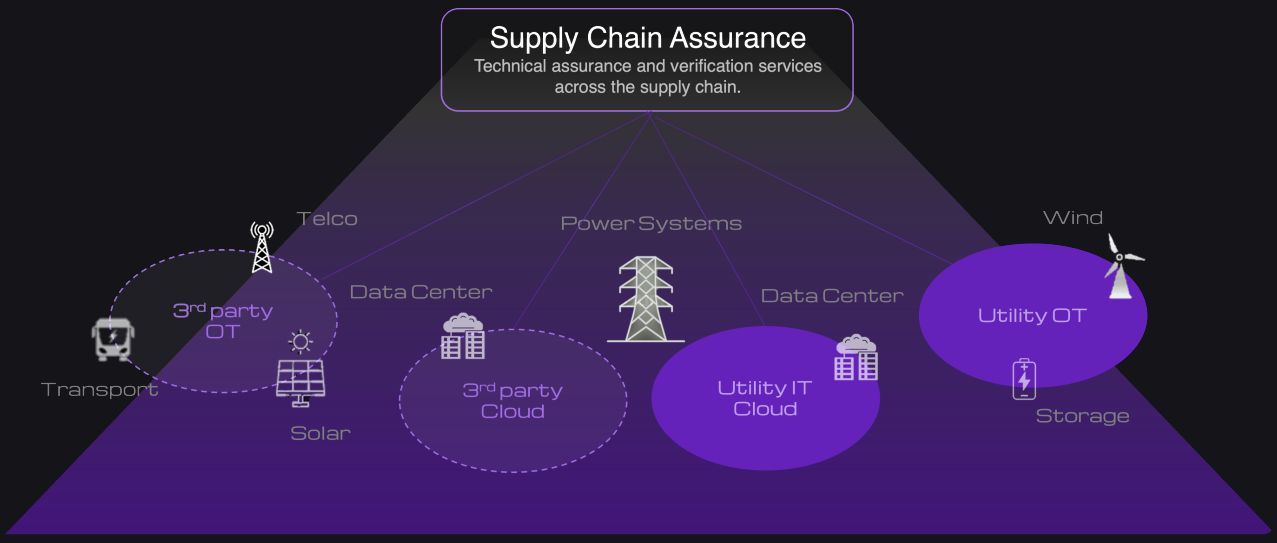
   Product images signed at source and verified at install, so what runs on the controller is provably what the vendor released — and any substitution is visible.

5. **Jurisdictional and personnel visibility**

   Ownership, control and influence assessed across vendors and their sub-components, and a record of who can touch the plant, from where, and on whose authority.

6. **Recovery you have actually tested**

   An offsite image repository and a restoration path proven before it is needed, rather than discovered during the incident that requires it.




*Technical assurance and verification services across the supply chain — power systems, utility IT and OT, cloud, telco and transport.*

HOW CAPA DELIVERS IT

# Three tiers of assurance

*A design baseline every operator needs, an entry-level vulnerability tier, and comprehensive assurance across the full chain of custody.*

Each tier is two-sided: obligations on the product vendor for what must be produced, signed and published at release, and the corresponding assurance for the operator at the site. What the vendor attests is what the operator verifies.

---

DESIGN BASELINE

## Supply chain mapping

*A governance requirement for operators to map their supply chains, quantify risk tolerance, and flag foreign interference risk.*

Mapping the supply chain is the baseline capability for every entity operating critical infrastructure assets. It is a systematic collation of the systems, software and hardware that sit within a critical asset or act as a critical operational dependency.

Aquila automates the creation of a digital registry for each product and version in the IT/OT estate, maps the key sub-components within each product, and lets asset managers or assurance providers run foreign interference (FOCI) checks across every element to meet new federal obligations.

---

SOLUTION 1 / ENTRY LEVEL

## Vulnerability assurance

*Entry-level assurance against known, published security vulnerabilities introduced in IT and OT systems.*

Vulnerabilities are identified through inspection of third-party dependencies and published advisories, with publishing and reporting against vulnerability-management SLAs.

FOR PRODUCT VENDORS

### Product vulnerability scanning

- Product SBOM inspection, release scans and attestation
- Continuous vulnerability scanning and triage management
- PSIRT VEX publishing and continuous reporting

FOR RENEWABLES OPERATORS

### Site vulnerability assurance

- Monitoring of product-vendor PSIRT VEX feeds for critical vulnerabilities
- Site triage of critical vulnerabilities against site particulars
- Escalation to SOC and patch-management processes

SOLUTION 2 / COMPREHENSIVE

# Complete supply chain assurance

*Comprehensive processes to manage vulnerabilities, introduced malware, FOCI risk and Fortify disaster-recovery scenarios.*

Full-chain assurance across product images and their third-party dependencies, covering the chain of custody from vendor to site, plus disaster recovery and restoration.

FOR PRODUCT VENDORS

### Product attestation

- Product SBOM inspection, release scans and attestation
- Continuous vulnerability scanning, triage and PSIRT VEX publishing

FOR RENEWABLES OPERATORS

### Product malware scanning

- Product image signing and chain-of-custody register for FOCI products
- Product image scanning and source-code attestation
- Offsite image repository backup

FOR RENEWABLES OPERATORS

### Site vulnerability assurance

- PSIRT monitoring across the product-vendor ecosystem
- VEX feed and SLA monitoring for critical vulnerabilities, with site triage

FOR RENEWABLES OPERATORS

### Site version management & recovery

- OT maintenance windows and priority patch schedules
- Site BOM registry, offsite image repository and restoration
- Chain of custody and personnel access assurance for FOCI products

---

DELIVERY

# In-house or fully managed

Assurance can be run in-house by the operator through the Aquila platform, or delivered as a turnkey CAPA managed service covering the baseline supply chain mapping and the ongoing assurance needed to meet the service levels required for IT and OT critical infrastructure operations — including the security operations capability described overleaf.

THE SUITE

# CAPA SecOps

*Assurance tells you what you have and whether it can be trusted. SecOps operates it — day to day, on the same inventory and the same evidence base.*

Aquila's supply chain assurance sits inside a wider security operations capability built for electricity-sector critical infrastructure. The modules share one asset registry, one vendor record and one audit trail, so a published vulnerability, a vendor access grant and an incident all resolve to the same product, version and site. Aquila and SecOps sit alongside CAPA GRM — governance, risk and maturity — on the same platform.

### Threat Intel and Vulnerabilities

Which weaknesses in your vendors' products actually matter to your sites, tracked from the day they are published until they are fixed.

### Personnel and Access

Who can reach your plant, on whose authority and from where — your own people and vendor technicians alike, with every session recorded.

### Threat Detection & Response

Watching the plant and the systems around it for signs of attack, with a tested plan for what happens when something is found.

ABOUT CAPA

CAPA Intelligence is an Australian based cybersecurity company servicing the global electricity / renewables sector, and global supply chains involved in supporting critical infrastructure. Our clients sit across the supply chain – governments, networks, retailers, system operators, IPPs, integrators and OEMs with operations in Australia and abroad.



Contact info@capaintelligence.com to arrange a demo

**capaintelligence.com**