PRODUCT BROCHURE

ASTRA
SECURING CRITICAL INFRASTRUCTURE

ASTRICS

THE OPERATIONAL INTELLIGENCE PLATFORM FOR INDUSTRIAL CYBERSECURITY

From Visibility to Understanding.

Industrial environments generate enormous volumes of data. Very little of it becomes understanding. ASTRICS turns industrial telemetry into one shared operational understanding — read by every capability in the platform.

ONE PLATFORM · ONE LANGUAGE · ONE SOURCE OF TRUTH

ASTRA CYBER SECURITY PTY LTD

THE PROBLEM

You can see every asset. You still can't answer the question.

When a critical decision has to be made, teams still reach for spreadsheets, manual processes and institutional knowledge to work out what the data actually means.

Visibility answers *what*. It rarely explains *why*.

Industrial operations are more than connected devices. Every asset supports a process. Every process supports a business outcome. Every decision carries operational, financial and regulatory consequences. Without context, even the most advanced telemetry is just data.

UNDERSTANDING MEANS KNOWING

- Why an asset exists
- Who owns it
- What depends on it
- What business impact it carries
- What process it supports
- How critical it is
- How it communicates
- Which regulatory obligations apply

Alerts ranked by severity, not consequence

Severity says how bad the bug is. It says nothing about what fails when the asset does.

Compliance rebuilt before every audit

Evidence assembled by hand from registers nobody trusts — then set aside until next year.

Every team keeps its own spreadsheet

Security, engineering, operations and compliance each hold a different version of the same estate. None of them agree.

THE SHIFT

The challenge isn't seeing more. It's understanding more.

Traditional platforms were built to answer one question — and they answer it well:

> “What happened on the network?”

Industrial organisations have always spoken different languages.

Security teams discuss vulnerabilities.
Engineers discuss assets.
Operations discuss uptime.
Executives discuss business risk.
Compliance teams discuss regulations.

ASTRICS brings them together through one operational model — and answers the questions that follow.

01 **What happened?**

02 **Why did it happen?**

03 **What operations are affected?**

04 **What business processes are impacted?**

05 **Who owns the affected assets?**

06 **What risks should be prioritised?**

07 **Which compliance obligations are involved?**

08 **What should happen next?**

That shift turns cybersecurity from an isolated technical function into an operational capability the whole organisation can use.

THE ASTRICS DIFFERENCE

Not another OT security platform.

Most OT platforms discover assets, decode protocols and generate alerts — then stop. ASTRICS starts where they stop.

TRADITIONAL OT SECURITY PLATFORMS		ASTRICS
Discover assets	→	**Understand operations**
Decode protocols	→	**Create operational context**
Generate alerts	→	**Deliver actionable intelligence**
Technical dashboards	→	**Business, operational and compliance intelligence**
Multiple disconnected tools	→	**One integrated operational platform**
Manual asset enrichment	→	**Continuous active enrichment**
Interaction visualisation	→	**Complete architecture and network diagrams**
Separate Syslog platform	→	**Native event log collection and analysis**
Compliance reporting	→	**Continuous compliance assurance**
Technical data	→	**Shared operational understanding**

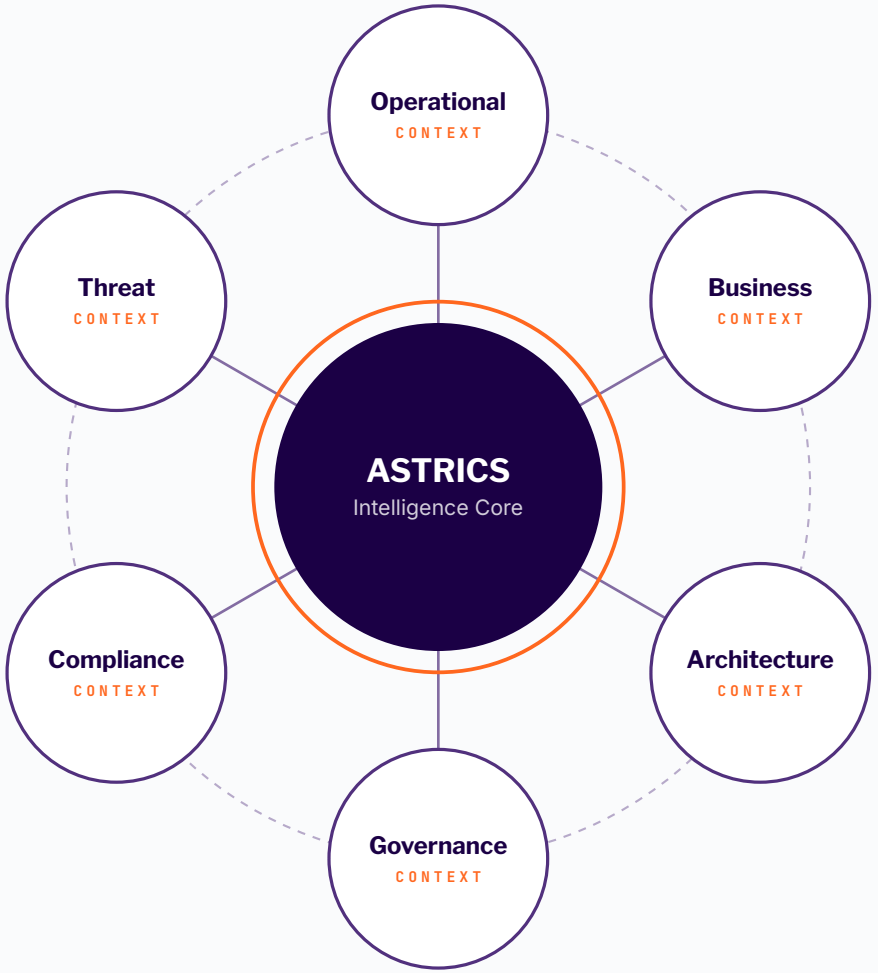
THE INTELLIGENCE CORE

Powered by the ASTRICS Intelligence Core.

Every capability in ASTRICS is built on a single intelligence foundation that continuously understands industrial assets, communications, operational processes, business dependencies and governance requirements. Rather than keeping separate datasets for security, operations, compliance and reporting, ASTRICS enriches one shared operational model — and every decision across the platform is made from it.

Operational	The role every asset plays within industrial processes.
Business	Ownership, criticality, business services and operational priorities.
Architecture	Where assets belong and how they communicate across zones and conduits.
Governance	Lifecycle status, accountability and organisational responsibility.
Compliance	Alignment with IEC 62443 and organisational requirements, through active enrichment.
Threat	Threats prioritised by operational impact — not technical severity alone.

One Intelligence Core.
One Operational Model.
One Trusted Source of Truth.

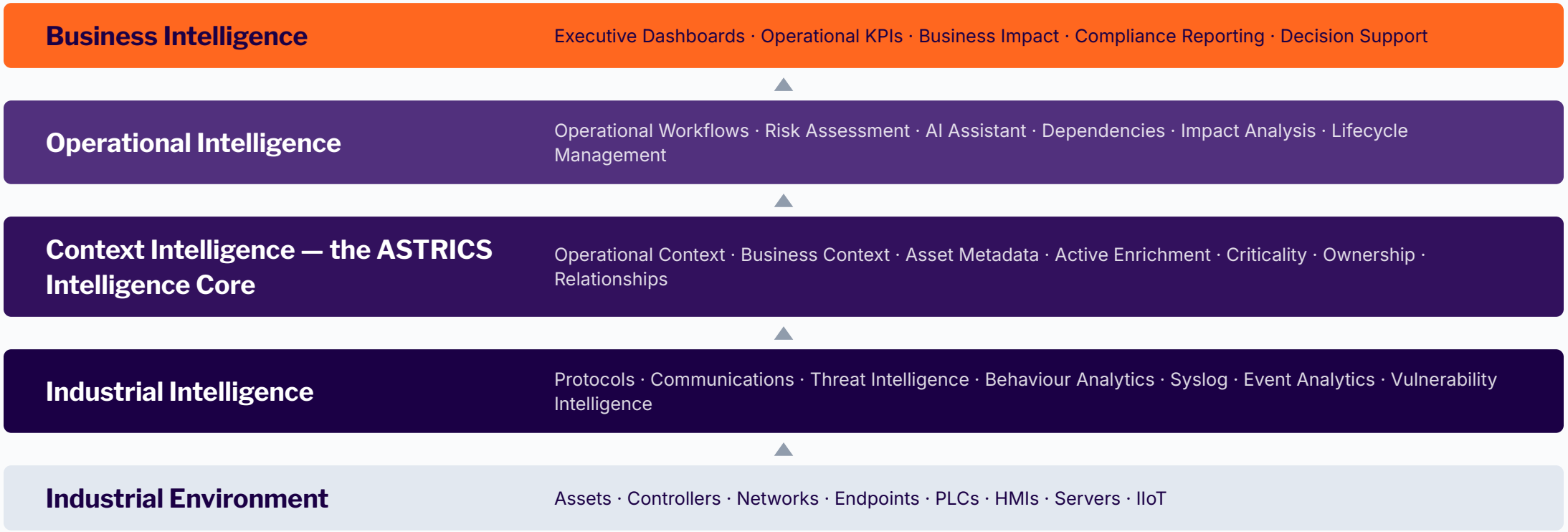


HOW IT WORKS

One understanding. Layered, not stitched.

ASTRICS layers intelligence progressively. Each layer reads the one beneath it and enriches it for the one above — raw industrial data in, operational decisions out.

RAW DATA → DECISIONS



Every dashboard, alert, workflow, compliance report and AI answer references exactly the same operational understanding.

THE PLATFORM

Four disciplines.
One operational model.

ASTRICS is organised the way industrial teams already work — and every discipline reads the same Intelligence Core.

1

Understand

Every asset is continuously enriched with operational, business, architecture, governance and compliance context — so ASTRICS knows what each device does for the plant, not just that it exists.

BUSINESS OUTCOME

One Operational Understanding

ASSET INVENTORY · ASSET PASSPORT · SINGLE LINE DIAGRAMS

2

Protect

Communications, protocol behaviour, events, threat and vulnerability intelligence are read inside the operational context they occur in — so every detection is ranked by consequence, not severity alone.

BUSINESS OUTCOME

One Security Posture

RISK QUEUE · EVENTS & SYSLOG

3

Orchestrate

An alert can become an investigation, a maintenance job, a risk assessment, a compliance review, a change request or an executive decision — all from the same understanding. Built-in AI answers in plain language.

BUSINESS OUTCOME

One Coordinated Response

OPERATIONAL ASSISTANT · WORKFLOWS

4

Govern & Assure

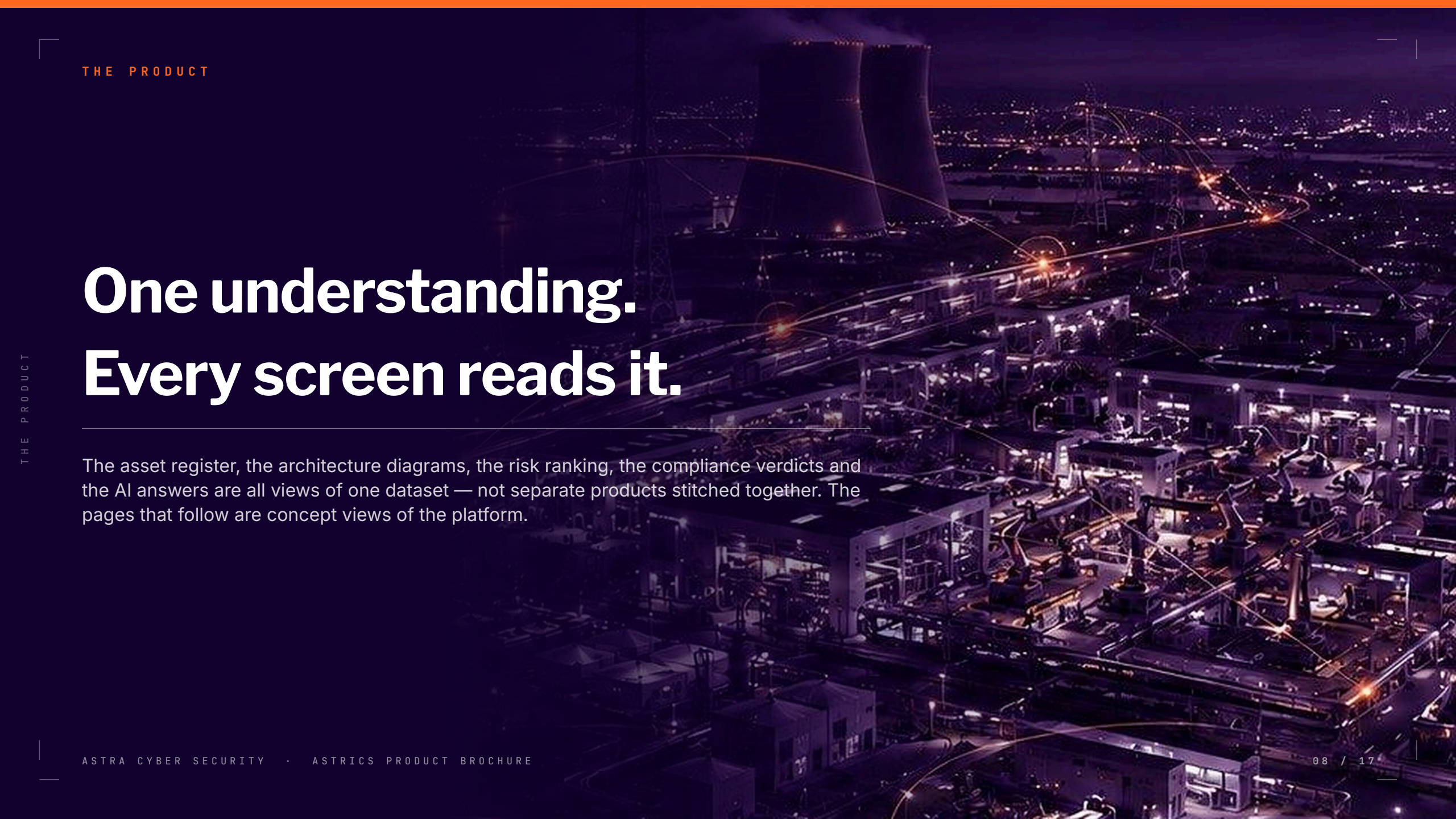
Architecture, asset lifecycle, operational risk, IEC 62443 alignment and compliance posture are validated continuously — governance embedded in everyday operations, not an annual reporting exercise.

BUSINESS OUTCOME

One Trusted Operational Record

COMPLIANCE · ZONES & CONDUITS · INCIDENTS

Everything becomes part of one continuous operational discipline.



One understanding. Every screen reads it.

The asset register, the architecture diagrams, the risk ranking, the compliance verdicts and the AI answers are all views of one dataset — not separate products stitched together. The pages that follow are concept views of the platform.

THE PRODUCT

BUSINESS INTELLIGENCE

Fleet Command

One posture number per obligation, across every site — built to answer “are we defensible today, and where are we not” in seconds, not in a reporting cycle.

1. **Readiness by chapter**
   Each control area scored and weighted by the assets actually in scope, so the weakest obligation is obvious.

2. **Impact-ranked attention list**
   What needs a decision today, with the plant consequence and the statutory clock beside it.

3. **Evidence age as a first-class metric**
   If evidence is stale, the posture is a guess — so freshness is measured and shown.

CONCEPT PRODUCT VIEW — NOT A PRODUCTION SCREENSHOT

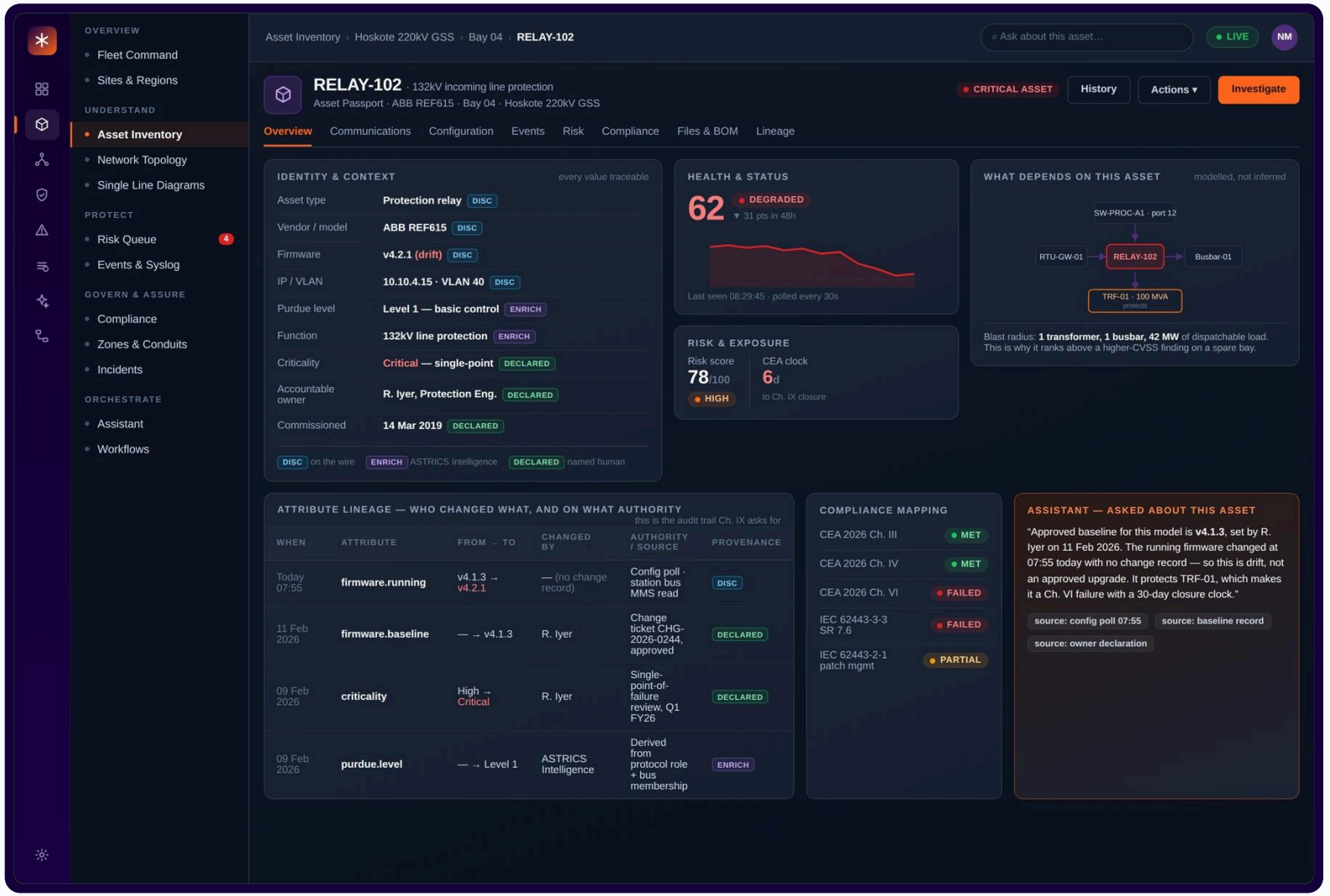
Asset Passport

One asset's complete operational record — and every value on it carries its source, so an auditor can follow any figure back to where it came from.

1. **Provenance on every attribute**
   Discovered on the wire, enriched by ASTRICS Intelligence, or declared by a named human owner.

2. **Blast radius, not just severity**
   What this asset protects and what fails with it — modelled from declared relationships.

3. **Attribute lineage**
   Who changed what, when, and on whose authority: the audit trail Chapter IX actually asks for.



CONCEPT PRODUCT VIEW — NOT A PRODUCTION SCREENSHOT

NETWORK INTELLIGENCE

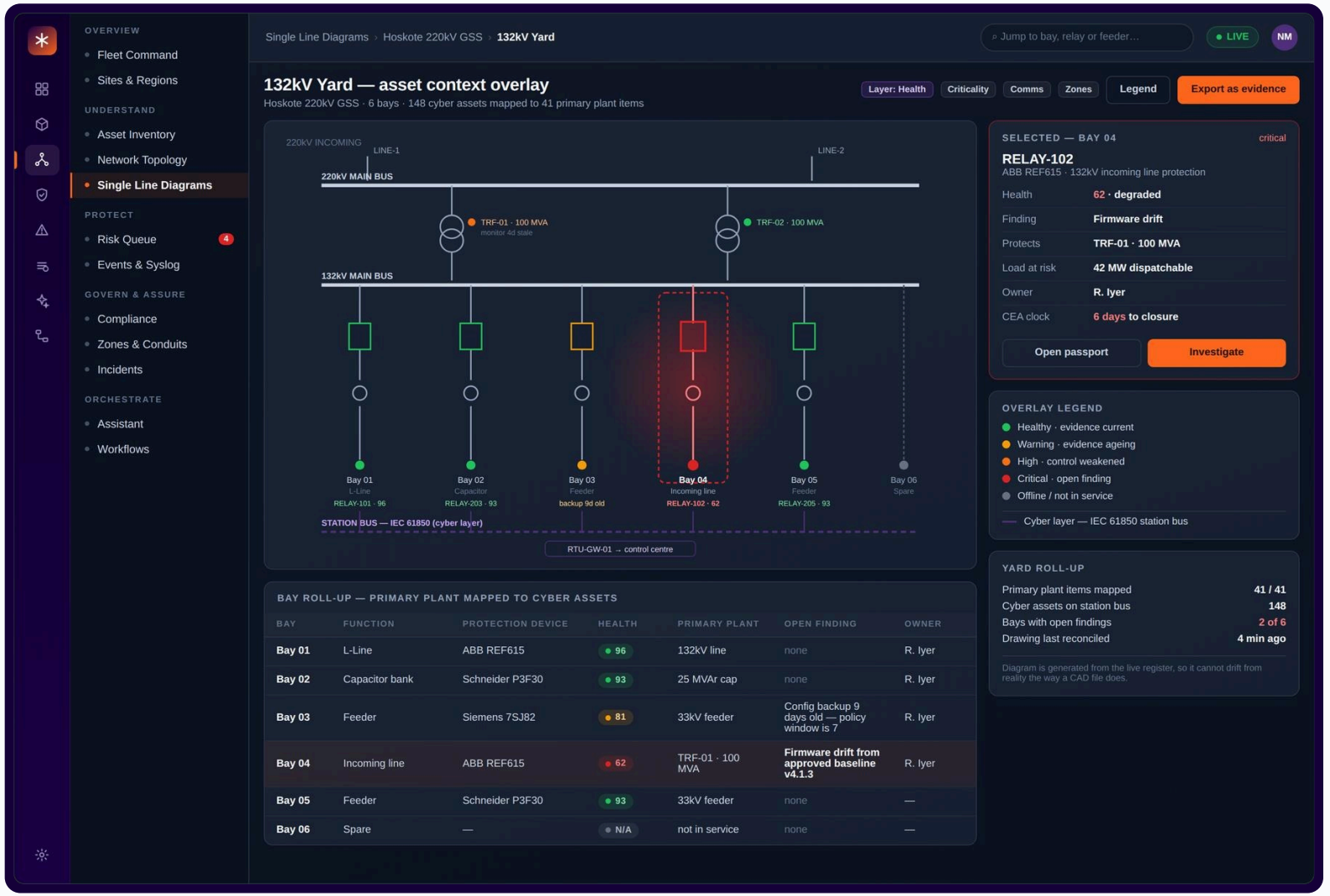
Single Line Diagram with Asset Context Overlay

The engineer's own drawing, alive. Cyber context is painted onto the layer operators already think in, so a finding reads as a bay, a transformer and a load.

1. **Generated from the live register**
   The diagram cannot drift from reality the way a CAD file left in a drawer does.

2. **Plant mapped to cyber assets**
   148 cyber assets tied to 41 primary plant items — the mapping is the deliverable.

3. **Exportable as evidence**
   The same view an engineer reads is the artefact an auditor accepts.



CONCEPT PRODUCT VIEW — NOT A PRODUCTION SCREENSHOT

GOVERN & ASSURE

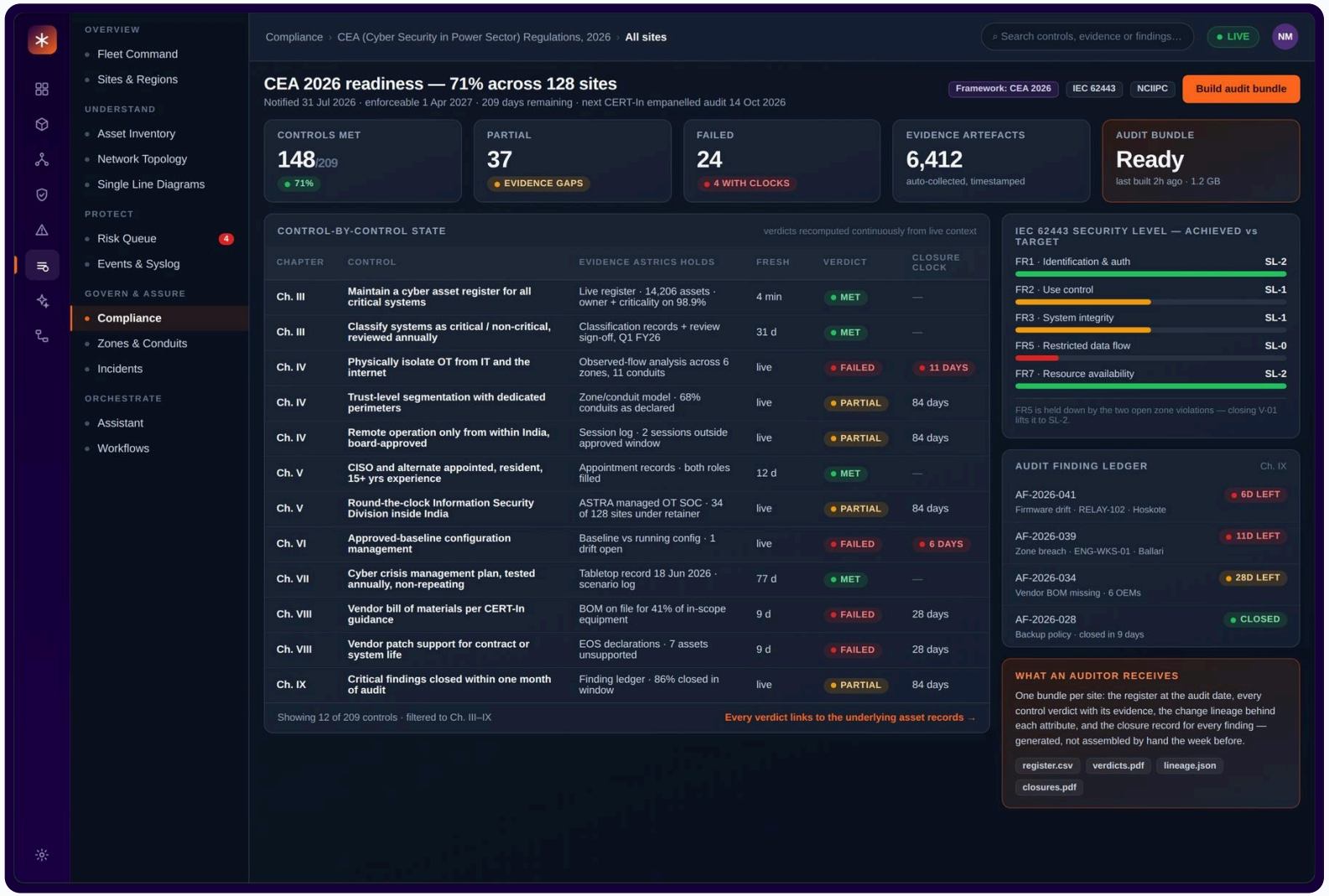
Compliance Console — CEA 2026 & IEC 62443

Compliance as a live state rather than an annual project: every control carries its current verdict, the evidence behind it, and the clock attached to any failure.

1. **Control-by-control verdicts**
   Recomputed continuously from live context, not reconstructed the week before an audit.

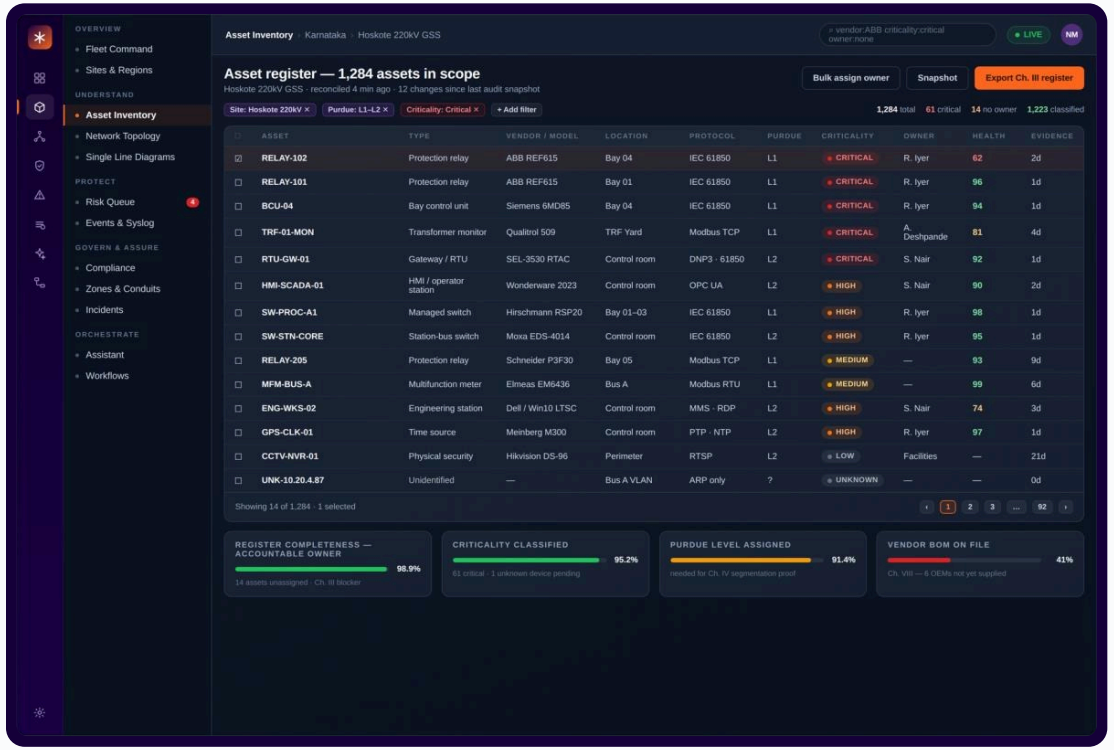
2. **Findings with statutory clocks**
   Chapter IX gives 30 days on critical findings — the ledger counts them down.

3. **The bundle an auditor receives**
   Register, verdicts, lineage and closures, generated rather than assembled by hand.



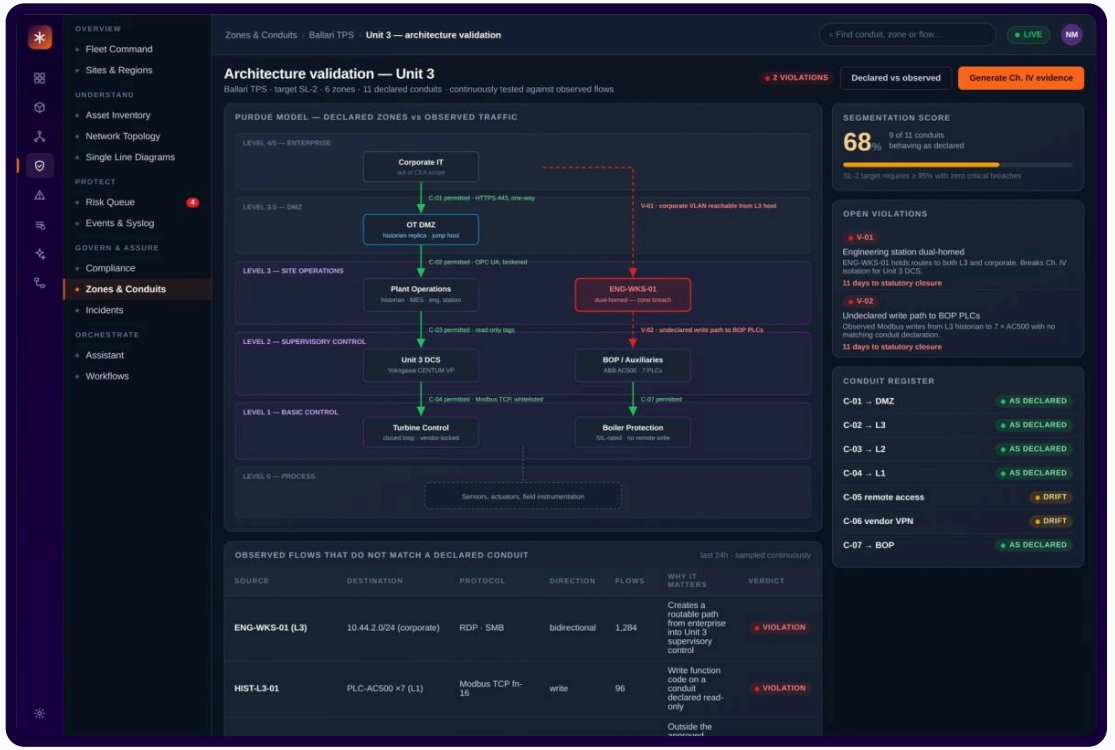
CONCEPT PRODUCT VIEW — NOT A PRODUCTION SCREENSHOT

The register, and the architecture it has to prove



Asset Inventory

The Chapter III register as a living object. Accountable owner and criticality are first-class columns because the regulation asks for them — and completeness against each field is tracked, since an incomplete register is a failed control.

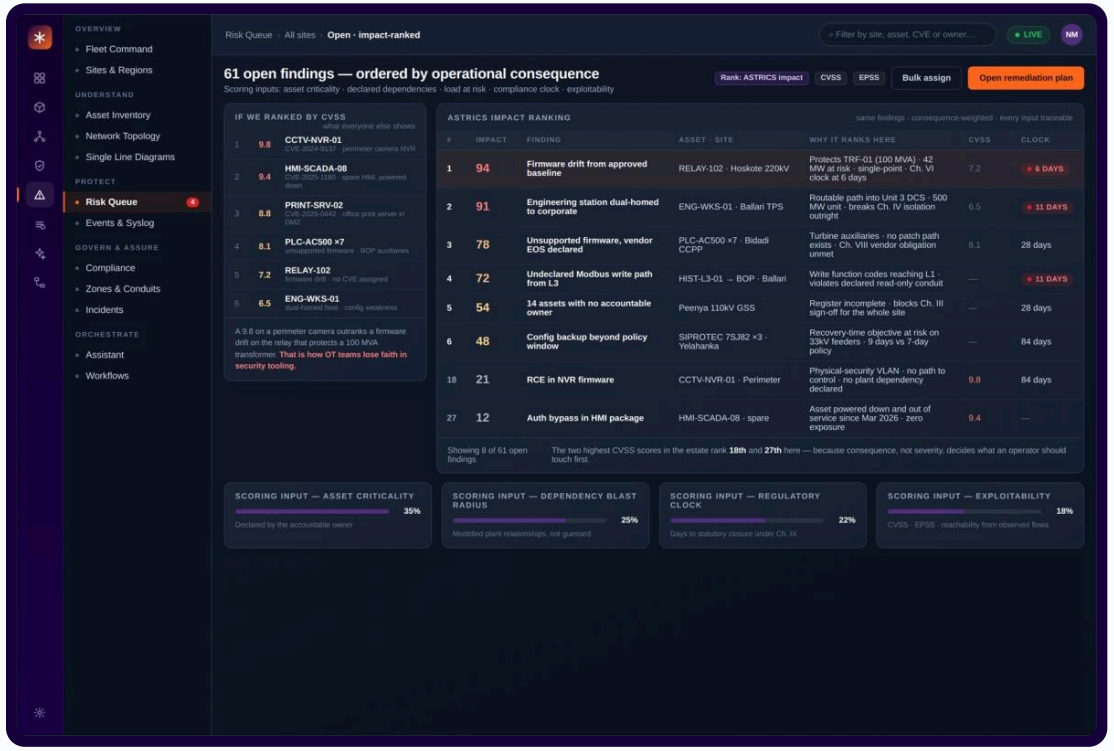


Zones & Conduits

Chapter IV asks an operator to prove trust-level segmentation, not describe it. Declared zones and permitted conduits are continuously tested against observed traffic, and every mismatch becomes a dated finding.

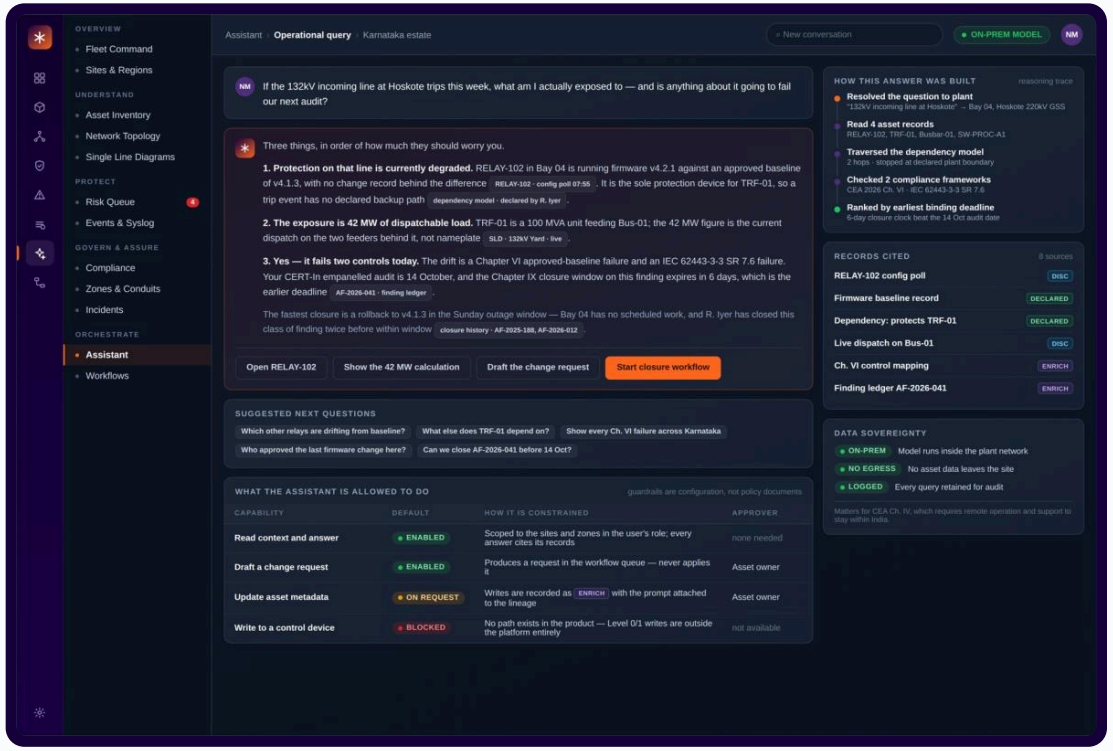
CONCEPT PRODUCT VIEWS — NOT PRODUCTION SCREENSHOTS

Deciding what to touch first — and asking why



Risk Queue

The same vulnerability data everyone has, ordered by what it would cost this operator. The two highest CVSS scores in the estate rank 18th and 27th here — because consequence, not severity, decides the work.

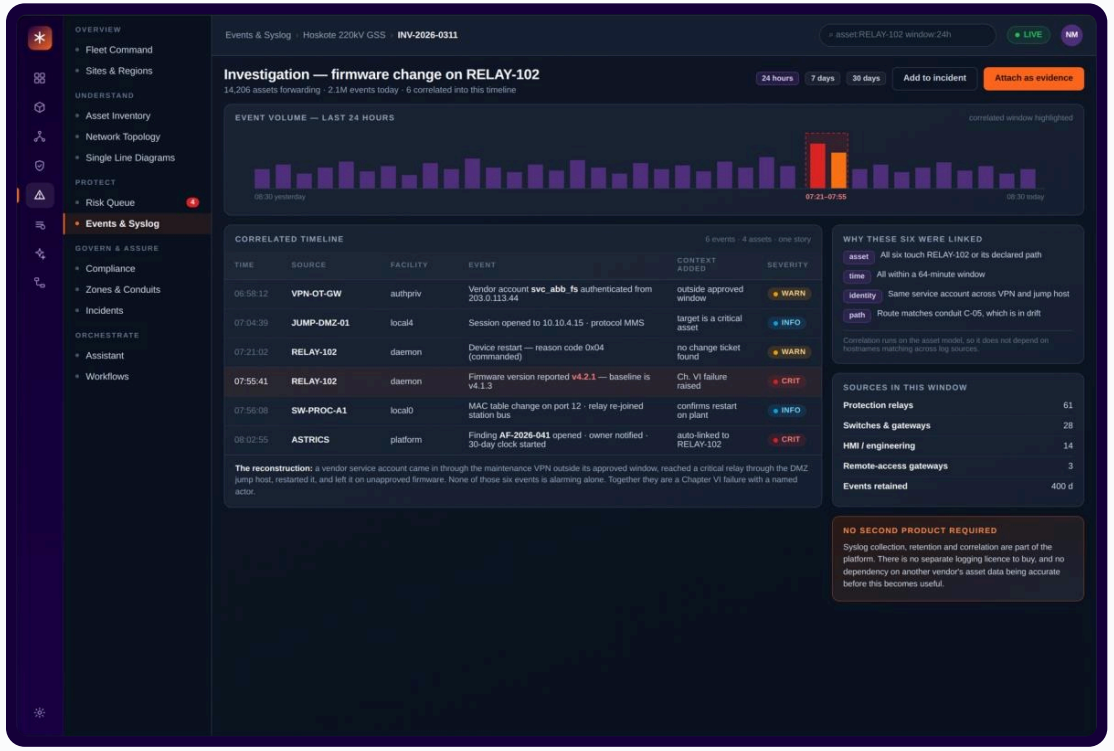


Operational Assistant

An on-premises assistant that cites the record behind every claim and shows the context it read. Writes to control devices are not a permission it can be granted — that path does not exist in the product.

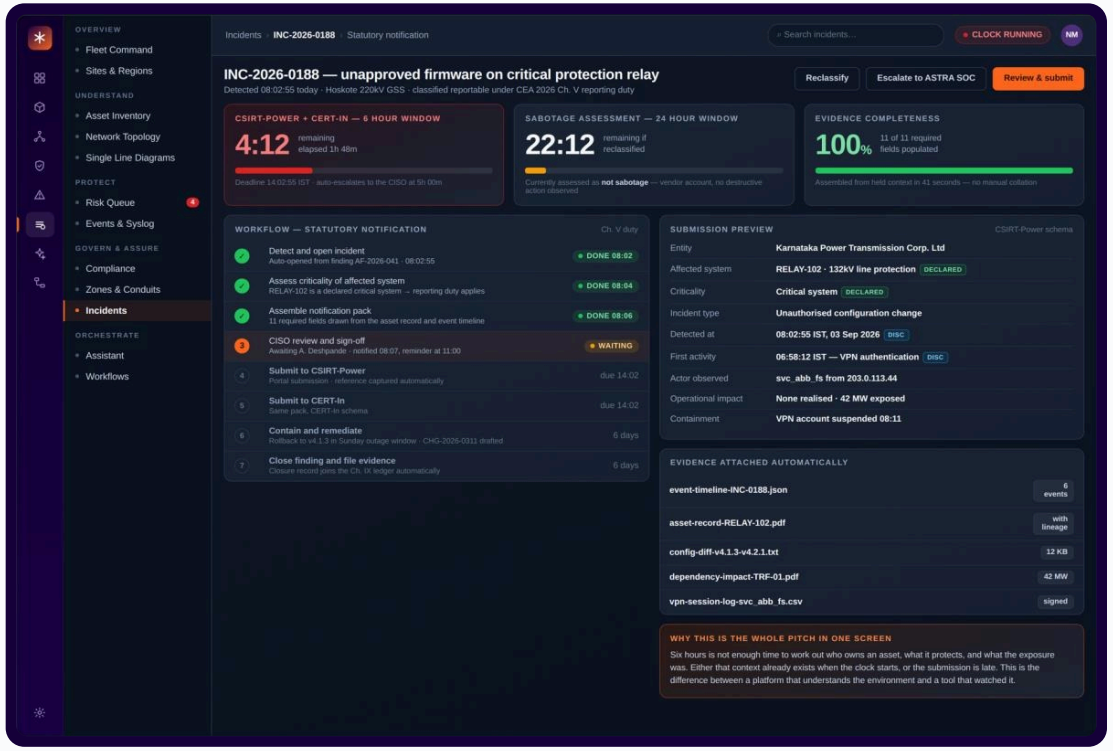
CONCEPT PRODUCT VIEWS — NOT PRODUCTION SCREENSHOTS

From six correlated events to a statutory submission



Events & Syslog

Native collection, retention and correlation — no second logging product, and no dependency on another vendor's asset data being right first. Correlation runs on the asset model, not on hostnames matching across log sources.



Statutory Incident Response

CEA 2026 allows six hours to notify CSIRT-Power and CERT-In. The clock, the workflow and the submission all run inside the platform, assembled from context already held.

CONCEPT PRODUCT VIEWS — NOT PRODUCTION SCREENSHOTS

DEPLOYMENT & LICENSING

Deploy it your way. License it simply.

DEPLOYMENT MODELS

- On-premises
- Private cloud
- Hybrid architectures
- Distributed multi-site, centrally managed

Air-gapped deployment is supported for qualifying environments — ask your ASTRICS team for site-specific guidance.

SIMPLIFIED LICENSING

- **No feature paywalls**
  Understand, Govern, Protect, Orchestrate and Assure travel together as one platform.
- **No per-tool sprawl**
  Built-in Syslog and event analytics replace the need for a separate logging product.
- **Scales with your estate**
  Licensing reflects sites and environments, not artificial technical caps.

Detailed licensing tiers and pricing are provided directly by your ASTRICS account team.

INTEGRATION

Sits alongside your stack — not in place of it.

Open, API-first integration lets ASTRICS share operational intelligence with the SIEM, ITSM and identity platforms your teams already use.

Confirmed integration partners and supported protocols are detailed in the current Technical Integration Guide, available on request.

ASTRA
SECURING CRITICAL INFRASTRUCTURE

Understand First. Secure Better.

Built in India. Proven in the field. Designed for the industrial world.

ONE PLATFORM · ONE LANGUAGE · ONE SOURCE OF TRUTH

Industrial cybersecurity isn't just about discovering assets or detecting threats. It's about understanding operations.

See ASTRICS against your own environment. Book a walkthrough with the ASTRICS team and bring one site's worth of questions.

REQUEST A DEMO →

astracyber.one · nikhil@astracyber.one

UNDERSTAND MORE · PROTECT SMARTER · OPERATE BETTER · GOVERN CONTINUOUSLY · SCALE WITH CONFIDENCE

Powered by ASTRICS Intelligence™

ASTRICS