

MORE TOOLS HAVE NOT GIVEN YOU MORE VISIBILITY

Which identities reached your control systems last night?

Your IGA knows who was entitled. Your OT monitoring knows a connection happened. Your historian knows a value changed. **None of them can tell you whether that behavior was normal for that identity.** The adversaries pre-positioning in critical infrastructure don't break in; they log in, with valid credentials, and wait. CINQUE is the correlation layer above the stack you already own: AI-native Unified Security Posture Observability.

THE RECONCILIATION NO OPERATOR RUNS

Every barrel, molecule and megawatt you move gets reconciled. **Access does not.** Entitlement is asserted in your role model; behavior is the only proof.

PERSONA	ENTITLED — PER RBAC	OBSERVED — PER CINQUE	VARIANCE	READ TOGETHER
OEM remote engineer	Vendor jump host only	→ Control network reached	BOUNDARY CROSSED	
Field telemetry account	Well-pad data, batch window	→ New scopes, off-window	SCOPE DRIFT	
Turnaround contractor	Read unit drawings	→ Read and bulk export	NEW EXPORT PATH	
Reliability AI agent	Recommend work orders	→ Recommend and create	FOUR-EYES BREAK	
Historian replication feed	Process data, continuous	→ Process data, continuous	RECONCILED	

Illustrative. Each variance above sits below the triage threshold of the console that owns it. It exists only once all five control points are read together.

Detection tells you what happened. Context tells you whether it was supposed to happen.

WHERE ENERGY OPERATORS POINT IT FIRST

The IT/OT boundary

Who, or what, is crossing from corporate toward control rooms, plants, and pipelines.

Vendors, integrators & OEMs

What contracted identities actually touched, from the jump host to the operations network and beyond it.

Non-human identities

Service accounts, Shadow AI, and the agents entering operational workflows, each baselined as a persona of its own.

Reporting readiness

When a risk is real, the full journey is attached: the story a 24-hour incident report needs.

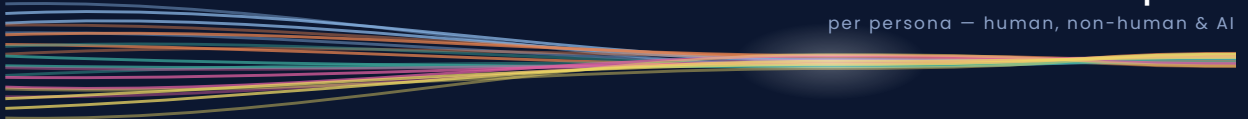
MAPPED TO WHAT YOUR REGULATORS AND ASSESSORS NOW EXPECT

THE EXPECTATION	WHO IS ASKING	WHAT CINQUE GIVES YOU
A current, defensible inventory of critical systems, identities and access	TSA SD Pipeline-2021-02 series · NERC CIP-002 / -004 · IEC 62443	Personas discovered from observed behavior — human, non-human and agentic — current by construction, not by refresh date.
Evidence the IT/OT boundary holds in practice, not just on the architecture diagram	TSA SDs (segmentation) · NERC CIP-005 · IEC 62443 zones & conduits	Every identity's observed journey across the boundary, reconciled against what its role asserts.
Continuous monitoring and detection inside the operational network	TSA SDs · NERC CIP-015 (internal network security monitoring) · CISA guidance	Behavioral baselines per persona across all five control points, Shadow AI and rogue service accounts included.
Evidence you can stand behind at assessment, to your insurer, and to the board	Your TSA-approved plan's annual assessment · your insurer · your board	A short list of correlated, business-contextualized risks with the full journey attached.

Sourcing: TSA SD Pipeline-2021-02 series requires segmentation, access control, continuous monitoring & detection, and patching under a TSA-approved plan assessed annually; NERC CIP-015 (approved 2025) requires internal network security monitoring. References current as of August 2026; obligations vary by segment, the direction toward continuous behavioral evidence does not.

FIVE THREADS. ONE FABRIC.

- IDENTITY
- DEVICE
- NETWORK
- APP
- DATA



One correlated risk picture

per persona — human, non-human & AI



Your data, handled like we mean it. You choose the export: limited, point-in-time, analyzed in an isolated environment, and deleted after your readout. Ask us for the data-handling summary — we are a security company; we expect the question.

THE CINQUE DISCOVERY WORKSHOP — COMPLIMENTARY

Bring one CSV. Leave with your reconciliation.

loomsecurity.io/requestdemo.html · info@loomsecurity.io

Book the
workshop

