CINQUE
BY LOOM SECURITY

FOR MANUFACTURING SECURITY LEADERS

MORE TOOLS HAVE NOT GIVEN YOU MORE VISIBILITY

Which identities touched the line last night?

Your security stack keeps growing, yet IT tools and OT tools still don't see each other. **None of them can tell you whether a vendor logging into a PLC, or a service account talking to a machine controller, is normal for that identity.** That's where real risk lives on a converged plant floor. CINQUE is the correlation layer above the tools you already own, IT and OT alike. It learns how every persona — human, non-human, and AI — behaves across **Identity, Device, Network, Application, and Data**, turning scattered alerts from your SASE, EDR, and OT monitoring tools into a short list of observable risks that actually need you.

FIVE THREADS. ONE FABRIC.

AI SECURITY MEANS TWO THINGS

AI FOR SECURITY

What every tool now claims

Machine learning added to a product to score, cluster, or summarize its own alerts — whether it's your MES, EDR, or network monitoring tool. Useful, but it is still one tool looking at one slice, and it cannot tell you whether an action **should have happened** on the plant floor.

SECURITY FOR THE AI YOU RUN

The part most tools skip

Your environment now runs copilots, predictive-maintenance agents, and autonomous robots that reason and access production systems at runtime. The question is simple: **Can you even see them? And what can they reach?**

CINQUE is AI-native, and it makes the AI already inside your environment **visible and contextual**. Shadow AI, engineering copilots, autonomous agents, and rogue service accounts on the plant floor show up as personas with observed behavior, measured against what is normal for that identity.

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

MAPPED TO WHERE OT SECURITY IS HEADING

IEC 62443 ZONE & CONDUIT REQUIREMENT		WHAT CINQUE'S CONTEXTUAL VISIBILITY GIVES YOU
Maintain an accurate inventory of assets across every zone and conduit	→	CINQUE discovers the personas actually active on your network — human, non-human, and AI — from observed behavior, not a static asset list that goes stale the day it's built.
Enforce identity and access control at every zone boundary	→	It correlates activity across Identity, Device, Network, Application, and Data into one journey per persona, so you can see exactly who, or what, is crossing from the corporate network onto the plant floor.
Monitor conduits for abnormal behavior, not just known signatures	→	Shadow AI, autonomous agents, and rogue service accounts surface as first-class personas, not blind spots between your IT stack and your OT monitoring.
Produce evidence for audits, insurers, and customer security reviews	→	Dozens of scattered signals across IT and OT become a short list of correlated, business-contextualized risk stories you can attest to.

Based on the ISA/IEC 62443 zone-and-conduit model for industrial automation and control systems, the working OT security standard across manufacturing. Defense-supply-chain manufacturers face a parallel deadline: **CMMC 2.0 Phase 2 begins November 10, 2026.**

SEE CINQUE ON YOUR ENVIRONMENT

Book a demo.
See your correlated risk picture.

Book a demo →

https://www.loomsecurity.io/requestdemo.html
info@loomsecurity.io

LOOM SECURITY