CINQUE
BY LOOM SECURITY

FOR OIL & GAS SECURITY LEADERS

MORE TOOLS HAVE NOT GIVEN YOU MORE VISIBILITY

Which identities touched SCADA last night?

Your posture stack keeps growing, yet each tool still sees only its own slice. **None of them can tell you whether an identity's behavior was normal.** That's where real risk lives in a contractor-run operation. CINQUE is the correlation layer above the tools you already own. It learns how every persona (human, non-human, and AI) behaves across **Identity, Device, Network, Application, and Data**. CINQUE turns scattered alerts into a short list of observable risks that actually need you.

FIVE THREADS. ONE FABRIC.

AI SECURITY MEANS TWO THINGS

Every tool now says it has AI security. It helps to separate what that can mean.

AI FOR SECURITY

What every tool now claims

Machine learning added to a product to score, cluster, or summarize its own alerts. Useful, but it is still one tool looking at one slice, and it cannot tell you whether an action **should have happened**.

SECURITY FOR THE AI YOU RUN

The part most tools skip

Your operations now run copilots, service accounts, and autonomous agents that reason and expand scope at runtime. The first question is simple: **can you even see them, and what they can reach?**

CINQUE is AI-native, and it makes the AI already inside your environment **visible and contextual**. Shadow AI, agents, and rogue service accounts 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 PIPELINE SECURITY IS HEADING

TSA SECURITY DIRECTIVE REQUIREMENT		WHAT CINQUE'S CONTEXTUAL VISIBILITY GIVES YOU
Maintain an inventory of critical cyber systems, refreshed on a set cycle	→	CINQUE discovers the personas actually active in your environment, human, non-human, and AI, from observed behavior rather than stale directory data.
Segment IT and OT so a compromise on one side cannot reach the other	→	It correlates activity across Identity, Device, Network, Application, and Data into one journey per persona, so you can see where control access concentrates.
Account for contractors, vendors, and AI that can reach control systems	→	Contractor accounts, vendor remote access, and autonomous agents surface as first-class personas, not blind spots between tools.
Produce assessment evidence you can stand behind each year	→	Dozens of scattered signals become a short list of correlated, business-contextualized risk stories you can attest to.

Based on TSA Security Directive Pipeline-2021-01 and -02 series requirements for TSA-designated critical pipeline owners and operators, and API Standard 1164, 3rd Edition. Directives are renewed annually and requirements may change, but the direction toward asset inventory, IT/OT segmentation, and continuous verification is clear.

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