CINQUE
BY LOOM SECURITY

FOR RAIL & TRANSPORTATION SECURITY LEADERS

MORE TOOLS HAVE NOT GIVEN YOU MORE VISIBILITY

Which identities touched the railroad last night?

The adversaries probing 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, learning what normal looks like for every identity across the enterprise, the yard, and the operations network.

FIVE THREADS. ONE FABRIC.

THE LEDGER A RAILROAD NEVER BALANCES

Every other ledger on the railroad 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
Wayside vendor tech	Signal telemetry only	→ **Dispatch** path reached	BOUNDARY CROSSED	●●●○○
Crew-ops service account	Crew boards, batch window	→ New scopes, **off-window**	SCOPE DRIFT	●○○●○
Engineering contractor	Read asset drawings	→ Read **and bulk export**	NEW EXPORT PATH	●○●○●
Maintenance AI agent	Recommend work orders	→ Recommend **and create**	FOUR-EYES BREAK	●○○●●
PTC back-office feed	Position reports, continuous	→ Position reports, 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 RAILROADS POINT IT FIRST

The IT/OT boundary
Who, or what, is crossing from corporate toward dispatch, signaling, and PTC.

Vendors & contractors
What contracted identities actually touched, on the operations network and beyond it.

Non-human identities
Service accounts, Shadow AI, and the agents entering rail 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.

EVIDENCE FOR THE PEOPLE WHO ASK

TSA SD 1580/82-2022-01 SERIES
Access control and continuous monitoring & detection for critical cyber systems, **evidenced from observed behavior**.

YOUR ANNUAL ASSESSMENT
The assessment plan asks whether controls work. Show how access is **actually used**, not how the diagram says it is.

YOUR INSURER & BOARD
A short list of correlated risks with **the full journey attached**, Shadow AI and rogue service accounts included.

TSA's rail directives (SD 1580/82-2022-01 series) require segmentation, access control, continuous monitoring & detection, and patching, under a plan assessed annually.

SEE CINQUE ON YOUR ENVIRONMENT

Book a demo. See your correlated risk picture.

Book a demo →

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

LOOM SECURITY

CORRELATE YOUR VISIBILITY. KNOW YOUR SECURITY POSTURE.