EventLake

For operations and engineering leadership, with security

OPERATIONAL TECHNOLOGY · ICS

The response that is correct on a laptop can be a safety event on a controller.

Isolating a compromised workstation is prudent. Isolating a controller mid-sequence is not, and no rollback repairs it.

THE ASYMMETRY

Availability is the safety control

In IT, containment costs minutes of disruption. Here it can cost a process, a batch, or a person — the order of priorities inverts.

THE CLASSIFICATION

Read from the asset, not the playbook

Where an asset carries a safety class, the platform proposes and a person with process authority decides — a property of the asset, not a relaxable setting.

THE PROPOSAL

Carries the full security case

The engineer deciding gets the computed scope, the basis and the evidence — not a softened summary.

What the platform will and will not do in a classified zone

the boundary is drawn, not implied

RUNS UNATTENDED

Observation and enrichment · alerting with the full path · blocking at the IT/OT boundary · isolating an engineering workstation · revoking a remote-access session.

PROPOSES ONLY

Anything touching a controller, a safety instrumented system, or a segment a process depends on. The proposal is recorded whether or not it is accepted.

Passive observation is the default in classified zones: span traffic and existing protocol data rather than active polling — a scan a controller mishandles is an outage you introduced looking for one.

WHERE THE VALUE ACTUALLY IS

The boundary, not the plant floor. Most OT incidents arrive through IT — a jump host, a vendor's remote session, an engineering laptop. That is where enforcement belongs and where it is safe.

Remote access as a first-class subject. Vendor and contractor sessions, scoped and expiring, re-evaluated rather than trusted for their duration.

An inventory you did not have. Passive observation produces the asset and dependency picture that makes a blast radius computable at all.

WHAT WE WILL NOT CLAIM

We do not observe below the agent, and in most of your plant there is no agent — firmware and controller-resident implants are outside what this platform sees. The compensating controls are attestation, supply-chain assurance and firmware integrity measurement.

A device with no agent and no path through an enforcement point is discovered, not covered.

START AT THE BOUNDARY

A session with operations in the room, not just security.

We will map your IT/OT boundary, name which asset classes carry a safety class, and agree what the platform may never do unattended — written down before anything is deployed.

Book a session

contact@eventlake.com

We ask for a work email and a phone number, and we tell you what we will do with them before you submit. We do not sell contact data, and one unsubscribe stops everything.

Paper 05 §5 · Paper 08 §3