The Lights Are Still On. For now.

Why your security stack cannot protect critical infrastructure — and what intelligence-led operations actually look like.

By José A. Cedeño · CloudCurrent LLC · 2025

After decades at the intersection of cybersecurity, strategy, and operations — across both public and private sectors — I've seen one pattern repeat itself with remarkable consistency:

> *Organizations are spending more on security than ever. And they are more exposed than ever.*

This isn't a budget problem. It's not a talent problem. It's a fragmentation problem — and in critical infrastructure, fragmentation doesn't cost you data. It costs you power.

The Stack You Built Is Working Against You

Your SIEM is firing alerts. Your EDR is logging endpoints. Your network scanners are churning through vulnerabilities. Your firewall is doing its job. But none of these tools are talking to each other in any meaningful way — and that silence is exactly where attackers live.

The dirty secret of enterprise security? Most teams aren't lacking data. They're drowning in it. What they're missing is intelligence — the ability to connect fragmented signals into a clear, unified picture of what's actually happening across their environment, right now.

In a corporate IT environment, that fragmentation is expensive and dangerous. In a power substation, a water treatment facility, or a national laboratory, it is catastrophic. The consequences of a missed signal are not a data breach notification and a credit monitoring service. They are grid failures, safety incidents, and disruptions to national energy capacity.

The OT Blind Spot Nobody Talks About

For years, the security industry has treated Operational Technology as an afterthought — a legacy environment that would eventually be modernized and folded into the IT security model. That approach has failed. Completely.

Nation-state actors understood this before we did. Volt Typhoon — the Chinese state-sponsored group identified by CISA, NSA, and the FBI — demonstrated the ability to pre-position inside OT networks for months, sometimes years, using Living off the Land techniques that generate no malware signatures, no anomalous traffic patterns, and no SIEM alerts. They look like normal network activity because they are using the tools that are already there.

> *The adversary doesn't need to break in. They're already inside — and your tools cannot see them.*

The reason is architectural. IT security tools are built around a threat model that assumes a network perimeter, identifiable malicious behavior, and systems that can be taken offline for remediation. OT environments violate all three assumptions. You cannot patch a substation relay during peak demand. You cannot take a SCADA controller offline for a security update. And a threat actor who understands this will use your operational constraints against you.

Asset Health Is the Foundation — Not an Afterthought

Before you can defend an environment, you have to know what's in it. This sounds obvious. In practice, it is the most consistently underestimated challenge in critical infrastructure security.

Most organizations operating power infrastructure have incomplete asset inventories. The assets that are inventoried are often out of date. Configuration drift — the gradual, undocumented divergence of a device from its known-good baseline — is endemic. And in OT environments, where a relay or RTU may have been installed fifteen years ago and never touched since, drift is not just a security problem. It is an operational reliability problem.

What asset health and management actually requires:

- ✔ Continuous, real-time visibility into every IT and OT asset — not a quarterly scan
- ✔ Automatic detection of configuration drift, with configurable thresholds and alerts
- ✔ A complete audit trail of every state change, across every node, over time
- ✔ The ability to visualize asset health directly on physical facility and substation maps
- ✔ Correlation of asset condition with security events — so you know if a degraded asset is also a targeted one

This is not a wish list. It is the minimum viable foundation for securing a power environment. Without it, every other security investment you make is built on sand.

What Unified Intelligence Actually Looks Like

The answer to fragmentation is not another tool. It is a fundamentally different approach to how security data is ingested, correlated, and presented to the people who have to act on it.

VStrike, developed by CloudCurrent, doesn't add to your stack. It makes your stack finally work. By ingesting and correlating data from your existing security ecosystem — SIEMs, EDRs, scanners, firewalls, OT sensors, physical IoT devices — VStrike synthesizes fragmented signals into a single, authoritative operational narrative. Real-time. Actionable. Clear.

But what distinguishes VStrike from a more capable SIEM is not integration breadth. It is the nature of the intelligence it produces:

True Asset Visibility
Know exactly what is in your environment — IT and OT — and whether your security policies are actually being enforced on every node, continuously.

Unified Situational Awareness
One coherent operational picture instead of ten competing dashboards. Events correlated across IT and OT simultaneously, mapped onto the physical layout of your facilities.

Behavioral Pattern of Life
Machine learning baselines that detect Living off the Land behavior — the kind of slow, low-signal activity that Volt Typhoon uses — that no signature-based tool can catch.

Event Replay & Storyboarding
When something happens, see exactly what happened, how it unfolded, and what the attacker touched — animated and replayable, with full timeline reconstruction across IT and OT.

Asset Health & Drift Detection
Every configuration change is recorded. Map-level visualization of drift. Correlation of degraded assets with active threats — so you know which vulnerabilities are being exploited right now.

Proven Operational Validation
At NNSA Imperial Catfish 2024, VStrike was the sole vendor to correctly reconstruct the full Volt Typhoon attack chain — 100% match to the Red/Blue Team out-brief. No other tool came close.

The Imperial Catfish Standard

Proof of concept exercises are common in this industry. Results like Imperial Catfish 2024 are not.

At the NNSA-sponsored exercise at Pacific Northwest National Laboratory — one of the most sophisticated national cyber exercises conducted in the United States — VStrike was invited

alongside other leading security platforms to observe and reconstruct a live red team operation simulating a Volt Typhoon attack against converged IT/OT infrastructure.

The result:

- ✔ VStrike was the sole vendor to correctly reconstruct the full attack chain
- ✔ 100% match to the Red/Blue Team out-brief — every event, every pivot, every target
- ✔ Volt Typhoon Living off the Land TTPs identified post-exercise — missed by every other tool
- ✔ Full reconstruction from IT reconnaissance through OT pivot to critical device targeting
- ✔ Defensive Digital Twin produced in days from Nozomi, Sepio, Eclypsium, and Cisco telemetry

> *"We were the only invited vendor that identified what happened, when, and how it happened — along with an animation showing the events." — VStrike Operational Report · Imperial Catfish 2024*

This is not a benchmark. It is a demonstration of what unified intelligence across IT and OT actually enables — and what its absence costs.

The Answer Isn't More Tools

If you are a CISO, security leader, or technology executive responsible for critical infrastructure — power generation, transmission, water, transportation, or national laboratory environments — the conversation you need to have is not about which new tool to buy.

It is about whether you can answer three questions right now:

1. Do you have real-time visibility into every IT and OT asset in your environment — including configuration drift and health status?
2. If an adversary has been inside your OT network for six months using only native tools, would you know?
3. If an incident occurred today, could you reconstruct exactly what happened, in what sequence, across both IT and OT — and show it to a decision-maker in a way they can understand?

If you cannot answer all three with confidence, you have a fragmentation problem — and no amount of additional point solutions will solve it. What you need is the intelligence layer that connects everything you have already bought and makes it finally work as a system.

The lights are still on. The question is whether you will know the moment someone decides to turn them off.

I'd welcome a direct conversation.