The Operational Blind Spot

Why asset health, unified intelligence, and operational visibility are the only things standing between your infrastructure and the adversary already inside it.

By José A. Cedeño · Cofresí Consulting Services · CloudCurrent Advisor · 2026

Somewhere in your infrastructure right now, a device is communicating that does not appear in your asset inventory. It has never been scanned. It has never had an agent installed. It generates no alerts. And it has been there — active, communicating, drifting from its last known configuration — for longer than you would be comfortable admitting to your board.

This is not a hypothetical. In every OT and IT network assessment I have conducted over 25 years across the Intelligence Community and the Department of Energy, this device exists. We call it the Dark Segment. And it is the single most reliable indicator of whether an organization's security posture is built on evidence — or assumption.

> *Your security tools are not failing. They are doing exactly what they were designed to do. The problem is that they were never designed to see the full environment.*

The Stack You Built Is Working Against You

The modern security stack is a triumph of procurement over architecture. Organizations have invested heavily — SIEMs, EDRs, firewalls, vulnerability scanners, network detection tools — and each tool, individually, performs as advertised. The SIEM fires alerts. The EDR logs endpoints. The scanner identifies vulnerabilities. The firewall enforces policy.

None of them are talking to each other in any meaningful way. And that silence — the gap between tools that were never designed to share a common operational picture — is exactly where sophisticated adversaries have learned to live.

The dirty secret of enterprise security is not that organizations lack data. They are drowning in it. What they are missing is intelligence — the ability to connect fragmented signals across IT

and OT simultaneously into a single, authoritative picture of what is actually happening across their environment, right now. Not what a tool believes is happening. What the wire proves.

Asset Health Is Not a Feature. It Is the Foundation.

Before an organization can defend its environment, it must know what is in it. This sounds obvious. In practice, it is the most consistently underestimated problem in critical infrastructure security — and in power environments, it is the one that gets people hurt.

Most organizations operating substations, generation facilities, and grid control networks have asset inventories that are incomplete, outdated, or both. Configuration drift — the gradual, undocumented divergence of a device from its known-good baseline — is endemic. A relay installed fifteen years ago and never touched since is not a static object. It is a system in continuous, unmonitored change.

In IT environments, configuration drift is an operational nuisance. In OT environments, it is simultaneously a security vulnerability and a reliability risk. The same undocumented change that opens a lateral movement path for an adversary may also be the change that causes a protection relay to misoperate under fault conditions. Security and operational continuity are not separate problems. They share the same root cause: incomplete visibility.

> **What real asset health and management requires:**
>
> ✔ Continuous, machine-speed visibility into every IT and OT asset — not a quarterly scan
>
> ✔ Automatic detection of configuration drift, with configurable thresholds and alerting
>
> ✔ A complete audit trail of every state change, across every node, over time
>
> ✔ Correlation of asset health with active security events — knowing which degraded assets are being targeted right now
>
> ✔ Visualization of asset condition directly on physical facility and substation maps
>
> *Without this foundation, every other security investment you make is built on assumption. An assumption is the adversary's most valuable asset.*

The OT Blind Spot Nation-States Exploit

For years, the security industry treated Operational Technology as a legacy environment that would eventually be modernized and folded into the IT security model. Meanwhile, nation-state actors studied OT environments with the patience and precision that only long-term strategic objectives produce.

Volt Typhoon — the People's Republic of China state-sponsored group identified by CISA, the NSA, and the FBI — demonstrated something the industry had theorized but not yet confronted at scale: the ability to pre-position inside OT networks for months, sometimes years, using only the tools and protocols already present in the environment. No malware signatures. No anomalous traffic patterns. No SIEM alerts. Living off the Land, in the literal sense — surviving entirely on the resources of the host environment.

> *The adversary does not need to break in. They are already inside. The question is whether you have the operational picture to see them.*

The reason these techniques work is architectural. IT security tools are built around a threat model that assumes identifiable malicious behavior, a network perimeter that can be defended, 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 an adversary who understands your operational constraints will use them against you — methodically, invisibly, and with a timeline measured in years rather than days.

The 200+ day average dwell time in OT environments is not a technology failure. It is the predictable outcome of monitoring architectures that were never designed for the environment they are deployed in — and asset health programs that stopped at the perimeter of the IT network.

What Unified Operational Intelligence Actually Looks Like

The answer to fragmentation is not a more capable SIEM. It is a fundamentally different approach to how security data is ingested, correlated, and presented — one that treats the IT/OT boundary not as an architectural limit but as precisely the place where visibility is most urgently needed.

VStrike, developed by CloudCurrent, approaches this differently. Rather than asking devices what they are — which requires agents, scans, and cooperation from hardware that may be decades old — VStrike asks what the wire proves they are doing. Network traffic cannot be faked. A PLC communicating via Modbus to an HMI generates packets whether or not any security tool is installed on it. If a device emits a single packet, VStrike sees it and places it on the operational map. No agents. No parsers. No Integration Tax.

The intelligence VStrike produces:

True Asset Visibility: Every IT and OT asset continuously mapped — including the Dark Segment your inventory missed. Configuration drift tracked against known-good baselines. Asset health correlated with active threats.

Unified Operational Picture: One coherent view across IT, OT, IoT, and Cloud — mapped onto the physical layout of your facilities. Not ten competing dashboards. One map. One truth.

Behavioral Pattern of Life: Machine learning baselines built for industrial stability. A controller that has communicated the same way for ten years deviating from that pattern is not noise — in OT, it is almost certainly significant.

Event Replay and Storyboarding: When something happens, see exactly what happened, in what sequence, across IT and OT simultaneously — animated and replayable, with full timeline reconstruction.

End Node Drift Detection: Every state change recorded. Map-level visualization of drift over configurable time spans. Know not just that something changed — know exactly what changed, when, and what it now connects to.

The Imperial Catfish Standard

Proof of concept exercises are common in this industry. Results like Imperial Catfish 2024 are not. At the NNSA-sponsored national cyber exercise at Pacific Northwest National Laboratory — one of the most rigorous operational security evaluations conducted in the United States — VStrike was the sole vendor invited to demonstrate unified IT/OT intelligence against a live red team simulating a Volt Typhoon attack against converged critical infrastructure.

The result:

✔ Sole vendor to correctly reconstruct the full Volt Typhoon attack chain

✔ 100% match to the Red/Blue Team out-brief — every event, every pivot, every targeted asset

✔ Living off the Land TTPs identified post-exercise — missed by every other tool present

✔ Full reconstruction from IT reconnaissance through credential abuse to OT pivot and critical device targeting

✔ Unified Operational Picture generated in days by mapping live telemetry from Nozomi, Sepio, Eclypsium, and Cisco.

"We were the only invited vendor that identified what happened, when, and how it happened — along with an animation showing the events." — VStrike

This is not a benchmark score. It is a demonstration of what unified intelligence across IT and OT actually enables — and what its absence costs when the adversary is already inside your environment and you have not yet closed the loop.

Three Questions Worth Asking Today

If you are a CISO, security leader, or technology executive responsible for 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 honestly answer three questions:

1. *Do you have real-time visibility into every IT and OT asset in your environment — including configuration drift and asset health status — right now, without running a scan?*
2. *If an adversary has been inside your OT network for six months using only native tools and legitimate protocols, would your current stack surface any evidence of that?*
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 act on?*

If you cannot answer all three with confidence, you have an operational blind spot. And no amount of additional point solutions will close it — because the problem is not the tools you have. It is the absence of an intelligence layer that connects them into a unified, actionable picture of your actual environment.

The answer is not more tools. It is finally making the ones you have worth what you paid for them.

I'd welcome a direct conversation.

ADVISORY DISCLOSURE

The author serves as a strategic advisor to CloudCurrent, the developer of VStrike. This relationship is disclosed in the interest of transparency. The views expressed represent the author's independent analysis.

ABOUT THE AUTHOR

José A. Cedeño is the founder of Cofresí Consulting Services, an IT strategy and cybersecurity advisory firm serving federal, critical infrastructure, and enterprise clients. He brings 25+ years of operator experience from the Intelligence Community and the Department of Energy, where he evaluated emerging technologies against the unforgiving reality of mission-critical operations — where failure is not an option and the margin for error is zero. He can be reached at info@cofresi-consulting.net or at cofresi-consulting.net.