WHITEPAPER · CRITICAL INFRASTRUCTURE SECURITY

# Modern IT/OT Threats Have Outgrown the Air Gap

How VStrike's Defensive Digital Twin and DeepTempo Behavioral Detection Eliminate the Blind Spots That Sophisticated Adversaries Exploit

CloudCurrent · Cofresí Consulting Services · 2026 · Business Confidential

## Proven at the National Level Before We Make the Case

Before detailing the problem, the architecture, or the compliance mapping, it is worth starting with what was validated in a real-world national exercise. In 2024, the National Nuclear Security Administration conducted Imperial Catfish 2024 at Pacific Northwest National Laboratory — a converged IT/OT scenario simulating a Volt Typhoon-style nation-state intrusion against critical infrastructure.

VStrike was the only invited vendor to produce unified situational awareness across the exercise. In a matter of days, the platform fused telemetry with various products and sensors deployed as part of the exercise scenario into a single Defensive Digital Twin. Post-exercise analysis matched the Red/Blue Team out-brief with 100% accuracy — identifying Volt Typhoon Living off the Land TTPs, TCP flooding, IP spoofing, credential abuse, lateral movement into OT systems, and final target acquisition. Every other tool in the exercise missed the full chain.

| 100% | Days | VoltTyphoon | FullChain |
|---|---|---|---|
| match to Red/Blue Team out-brief | to fuse sensor's analytical results | LotL TTPs detected — missed by all others | IT recon → OT pivot → critical device targeting |

> *"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 · Pacific Northwest National Laboratory*

The active engagements that followed from Imperial Catfish speak to what the exercise validated:

| Organisation | Status |
|---|---|
| **DOE** | Active Proof of Concept following Imperial Catfish 2024 success |
| **TAC — Columbia, MD** | Live implementation Spring 2026: transport, water & energy sector |

## The Assumption Problem

Somewhere on a transmission substation network right now, a decommissioned engineering workstation is still running. It has been online for 847 days. It has never been scanned, never had an agent installed, and appears nowhere in any asset inventory or CIP-010 baseline. Last Tuesday, it made its first outbound connection — to an IP address associated with a known APT group.

No alert fired. No one noticed. Your firewall never saw it.

This is not a hypothetical. This is the **Dark Segment** — and it exists in every OT and IT network we have assessed, without exception. In a NERC CIP-regulated environment, a Dark Segment asset is not just a security risk. It is an undetected BES Cyber Asset: undocumented, unprotected, and outside your Electronic Security Perimeter by definition.

> *"The average dwell time in OT environments before detection is 200+ days. In a BES environment, that is 200+ days of undocumented exposure inside your Electronic Security Perimeter."*

| 200+ | 100% | 45+ |
|---|---|---|
| Average OT dwell time before detection (days) | Of networks assessed contain at least one Dark Segment asset | Average security tools per enterprise — adding noise without a fusion layer |

## Why Your Security Stack Is Forbidden on the Substation Floor

OT security has an uncomfortable paradox at its core: the tools that provide the deepest visibility in IT environments are precisely the ones most likely to cause a production outage in OT. Active scanners have crashed legacy protective relays. EDR agents have introduced latency into millisecond-sensitive control loops. The result is an unspoken rule across most substations and control centers — the security team does not touch the OT network.

The substation floor becomes a black box. NERC CIP-015 requires operators to implement Internal Network Security Monitoring across BES Cyber Systems, but the passive requirement in CIP-015 R1.1 exists precisely because active monitoring tools cannot safely operate in these environments. The compliance obligation exists; the safe means of satisfying it has historically not.

## The Air Gap Is Not What You Think

Most organizations believe physical or logical separation between their corporate IT network and OT production zone provides a reliable security barrier. In practice, this assumption fails consistently and silently. Each of the following scenarios creates an undocumented Electronic Access Point under CIP-005 — a crossing that exists in your environment but not in your compliance documentation.

| Dual-homed engineering laptops | Rogue wireless access points |
|---|---|

| | |
|---|---|
| Maintenance laptops carried in during site visits physically bridge the IT/OT boundary — bypassing every perimeter control. | APs installed for operational convenience create undocumented ESP crossings that persist long after the technician leaves. |
| **Misconfigured VLANs**<br>Legacy segments create invisible paths between IT and OT domains — traversable by adversaries, invisible to both teams. | **Decommissioned assets left online**<br>Equipment assumed offline continues running on the OT subnet: unpatched, unlisted in CIP-010 baselines, outside the documented ESP. |

> *The gap between the network that exists and the network you think you have is where sophisticated adversaries — and the Volt Typhoon TTPs validated at Imperial Catfish — operate.*

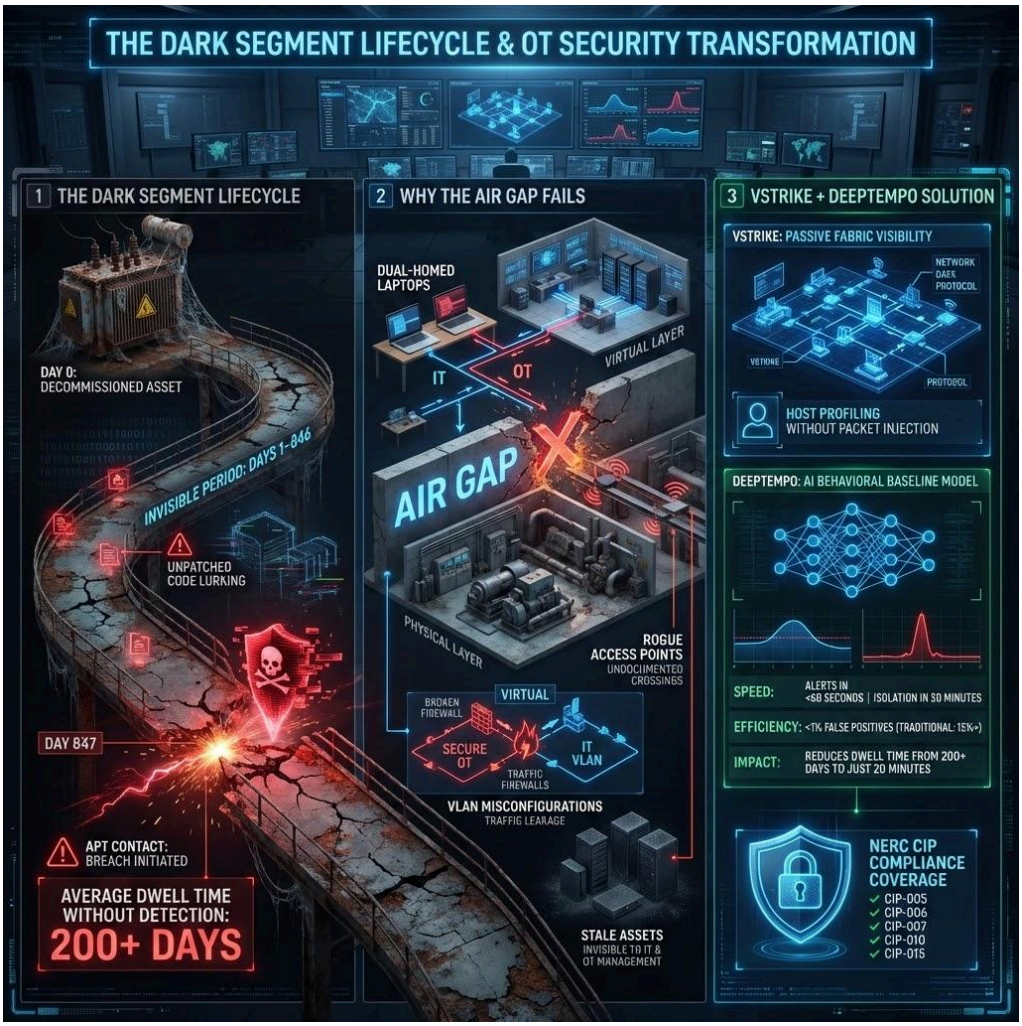


*Figure 1 — VStrike Defensive Digital Twin: Fusion Architecture & Validated Outcomes*

## The VStrike Platform: Defensive Digital Twin for IT/OT Environments

VStrike is not a passive network sniffer and it does not replace your existing tools. It is the fusion layer that sits above them — ingesting telemetry from your OT monitors, IT security stack,

physical IoT sensors, and cloud environments, then transforming those fragmented outputs into a single unified operational picture: the Defensive Digital Twin.

The fundamental question VStrike answers is not *"what does a device report about itself?"* — which requires agents and the device's cooperation. It is: *"what does the full picture of the wire prove this environment is actually doing?"* Network behavior cannot be faked across a fused multi-source timeline.

| | |
|---|---|
| **Multi-Domain Sensor Fusion**<br>Native IT (SNMP/Syslog) and OT (Modbus, DNP3, IEC 61850) ingestion — plus IoT environmental sensors — on one master timeline. No separate OT collector required. | **3D Storyboarding & Event Replay**<br>Maps events onto a 3D physical model of your environment. Play and replay any incident with full animation. Validated 100% accurate at Imperial Catfish 2024 — the only tool to reconstruct the full attack chain. |
| **Shadow Asset Discovery**<br>Automatically surfaces unauthorized and unmonitored devices that traditional tools never see — the rogue PLC, the forgotten workstation. The core response to the Dark Segment problem. | **Behavioral Baseline (Pattern of Life)**<br>ML continuously characterizes normal device behavior. Deviations trigger immediately — catching Living off the Land techniques and nation-state TTPs before signatures exist. |
| **Defensive Digital Twin**<br>A continuously updated, correlated model of your entire cyber-physical environment. Sits above your existing tools — Nozomi, Cisco, Sepio, Eclypsium, DeepTempo — and transforms their fragmented outputs into one unified picture. | **End-Node Drift Detection**<br>Every asset state change is recorded. Configurable drift reports over any time span. Map-level visualization flags every node that deviated beyond threshold — critical for SCADA and substation asset integrity. |
| **Air-Gap & Flyaway Deployment**<br>Flyaway kit architecture for forward-deployed field environments, air-gapped national laboratories, and classified OT networks. No external connectivity required — fully sovereign, fully operational. | **Open Plugin Architecture**<br>20+ native integrations: Nozomi, Sepio, Eclypsium, Cisco, Splunk, AWS, Azure, Trellix, Nessus, DeepTempo. REST/streaming APIs, RBAC, and enterprise auth included. DOE-specific and classified data sources fully supported. |

## The Intelligence Layer: DeepTempo Behavioral Detection

VStrike maps the *where*. DeepTempo provides the *how*.

OT environments have a property that makes behavioral detection uniquely powerful: stability. A well-running protective relay does the same thing, on the same schedule, to the same endpoints, for years. Unlike threshold-based anomaly tools that evaluate individual events in isolation, DeepTempo's foundation model uses zero-shot detection — identifying attacks immediately upon deployment without requiring an extended baseline period, because it recognizes the structural signatures of malicious intent rather than deviations from a learned norm.

This distinction matters operationally. Organizations cannot afford weeks of tuning before a detection system becomes effective. DeepTempo detected sophisticated attack patterns across diverse ecosystems — without retraining for each environment.

| IT ENVIRONMENTS | OT ENVIRONMENTS |
|---|---|
| **Noisy baselines** | **Detection weapon** |
| Users change behavior constantly, generating a high volume of anomalies requiring constant tuning. Traditional tools produce 15%+ false positive rates. Behavioral detection is valuable but operationally costly. | A relay that has communicated the same way for ten years deviating from that pattern is not noise — it is either an attack or a fault. DeepTempo's zero-shot detection operates below 1% false positive rates, built for industrial behavioral patterns from the ground up. |

### High-fidelity anomaly detection examples

DeepTempo surfaces deviations that single-event rules miss: a dormant safety controller initiating an outbound connection after 847 days of silence; a PLC receiving commands from an IP address it has never communicated with; an Engineering Workstation querying assets outside its normal operational zone; a protective relay behaving anomalously following a physical access event — the correlated physical and cyber kill chain that signature tools cannot see.

## Live Scenario: The Dark Segment

The following scenario illustrates what detection and response looks like when VStrike and DeepTempo are deployed at a NERC CIP-regulated transmission substation. Note particularly T+8 min: this is where VStrike's 3D Storyboarding engine assembles the attack as a replayable incident animation — the same capability that produced a 100% accurate reconstruction at Imperial Catfish 2024.

| Time | Event | Detail |
|---|---|---|
| **Day 0** | **Decommission** | Production line decommissioned. Equipment physically removed. Network switch left powered on. No one turns off the breaker. |
| **Days 1–846** | **Dark Segment** | Legacy HMI continues running on OT subnet. Invisible to IT — no agent, no CMDB entry, not in CIP-010 baseline. Invisible to OT team — assumed offline. Unpatched for 2+ years. Outside documented ESP boundary. |
| **Day 847** | **Detection** | VStrike's Pattern of Life ML detects the first anomalous outbound connection from a dormant device. DeepTempo flags: baseline broken, destination IP matches known APT infrastructure. Alert fires in under 60 seconds. |
| **T + 5 min** | **Lateral exposure** | VStrike’s live topology map surfaces the compromised HMI’s legacy network path to active production PLCs on the adjacent subnet. Undocumented ESP crossing confirmed and visualized. CIP-005 gap identified. |
| **T + 8 min** | **Enrichment** | VStrike 3D Storyboard assembles the full attack timeline — device identity, location, network exposure, C2 destination, lateral |

| | | |
|---|---|---|
| | | movement path, CIP asset classification — as a replayable incident animation. |
| **T + 20 min** | **Containment** | Device isolated, network path severed, incident contained. Production unaffected. CIP-015 R2 forensic record initiated. Immutable evidence chain preserved for audit. |

**WITHOUT VSTRIKE + DEEPTEMPO**

Devices remain invisible. Attack progresses undetected. CIP-005 undocumented crossing is never identified. Discovery occurs weeks or months later — after lateral movement to production BES Cyber Assets. No forensic timeline exists. NERC audit exposure is compounded by the inability to reconstruct what happened or when.

## NERC CIP Compliance Posture

VStrike's architecture addresses NERC CIP requirements at every layer. The platform was designed for BES environments, not adapted from an IT security tool. The passive ingestion model satisfies CIP-015's monitoring obligations without the operational risk that active tools introduce. End-node drift detection and the live network topology map directly support CIP-010 configuration baseline requirements. The 3D Storyboard provides an immutable, replayable forensic timeline for CIP-015 R2 evidence.

| Standard | Requirement | VStrike Posture |
|---|---|---|
| **CIP-005** | ESP definition · EAP documentation | Minimal EAP footprint · ESP perimeter defined · all crossings documented via live network map |
| **CIP-006** | Physical security · EACMS | Physical IoT sensors classified as EACMS · isolated VLAN · passive telemetry only |
| **CIP-007** | No write to BES Cyber Assets · patch | VStrike issues no commands to BES Cyber Assets · enforcement via network infrastructure · patch via verified secure media |
| **CIP-010** | Configuration change management · baseline | Automated end-node drift detection · scheduled + event-triggered · config drift reports · near real-time topology map |
| **CIP-015** | INSM · immutable log · forensic evidence | Pattern of Life ML satisfies anomaly detection requirement · 3D Storyboard provides immutable forensic timeline · unified physical + cyber evidence |

## The Strategic Outcome

**REPLACING ASSUMPTIONS WITH EVIDENCE**

For years, BES operators have accepted a false choice: accept the visibility gaps created by monitoring tools too dangerous to deploy in OT environments, or risk the operational disruptions those tools introduce. VStrike and DeepTempo eliminates this trade-off entirely — and Imperial Catfish proved it in a live national exercise before any utility had to take the risk themselves.

The Defensive Digital Twin means the security team can finally operate on the substation floor without IT/OT conflict. Multi-source fusion means the OT team finally has a shared language with security analysts. The 3D Storyboarding engine means that when something truly anomalous occurs — an attack, a fault, a Dark Segment asset coming alive — it surfaces immediately, with a replayable timeline showing exactly what happened and in what sequence, before it reaches your crown jewel BES Cyber Assets.

The Dark Segment is not a technology problem. It is an assumption problem. Organizations assume the air gap holds, that decommissioned means offline, that unmonitored means safe. VStrike replaces assumptions with evidence. If it is on the wire, it is on the map. If it crosses the ESP, it is documented. If it deviates from baseline, it is flagged. And if it needs to be reconstructed for an audit or an incident brief, it can be replayed — accurately — as it actually happened.

The organizations that will avoid the next Colonial Pipeline, the next Ukraine grid incident, the next water treatment compromise are the ones that stopped trusting their asset inventory and started trusting their fused, correlated, continuously updated picture of the wire — and their compliance posture.