AFCEA TECHNET CYBER 2026 · BALTIMORE · JUNE 2026

Building towards full autonomy with Visualization, Workflow and AI

See the system deployed at the Technical Advancement Center
https://thetac.tech/

EVAN POWELL

DeepTempo · LogLM & Vigil SOC

AARON BOTELER

CloudCurrent · vStrike Fusion Layer

deeptempo.ai · cloudcurrent.biz · vigilsoc.org

CrowdCurrent and DeepTempo: Winning teams collaborating

100%

of a Volt Typhoon attack chain rebuilt

Reconstructed in the NNSA Imperial Catfish 2024 exercise.

CrowdCurrent: Imperial Catfish 2024 Winner

DeepTempo: DevCon ‘25 Blue Team CTF Winner

95%+

fewer false alarms

Introduced by the TAC and now delivering complete solutions

10×

faster to spot a real attack

THE PROBLEM

Mythos is just the beginning.
Expect 100-1M x more intelligence, scope, & speed by a broader set of AI-enabled attackers.

We all know we need to get to machine speed with autonomy. But not *too much* autonomy, too soon.

We bring together context, visualization, identification, and transparent automation that users control.

Users capture their radically accelerated and more intelligent OODA loops.

National Cyber Innovation Forum

PRESIDENTIAL ACTIONS

PROMOTING ADVANCED ARTIFICIAL INTELLIGENCE INNOVATION AND SECURITY

Executive Orders | June 2, 2026

NIST Internal Report
NIST IR 8596 iprd

Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile)

NIST Community Profile

Initial Preliminary Draft

Katerina Megas
Barbara Cuthill
Applied Cybersecurity Division
Information Technology Laboratory

Marissa Dotter
Michael Garris
Ishika Khemani
Bronwyn Patrick
Noah Schiro
Julie Nethery Snyder
Mohammad Zarei
National Cybersecurity Center of Excellence
MITRE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8596.iprd

December 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting NIST Director and Acting Under Secretary of Commerce for Standards and Technology

Three ways OT needs AI and open source

01

Patching? Are we talking about *patching*?

While much of the focus “post Mythos” has been on patching vulnerabilities - that is even less practical in OT environments.

02

OT environments are special

Cloud Current’s vStrike is the best solution for seeing *all* types of OT systems, capturing their interactions, and making it visible for human operators and for AI.

03

Labor shortage

AI can implement useful best practices across the global. This is collective defense PLUS open source led cost savings.

WHERE LEGACY STACKS BREAK DOWN

Three gaps the adversary uses every day

01

Signature-bound detection

Rules and signatures only catch what someone already saw and wrote down. AI-driven polymorphic threats, living-off-the-land techniques, and slow-burn C2 sail past.

02

Alerts without operational context

An IP and a port tell an analyst very little. Which asset is this? Which segment? Which mission system? Without the network picture, triage stalls.

03

Human-only response

Analysts pivot between consoles, copy IOCs by hand, and wait on tickets while an attacker pivots in seconds. Time to contain is measured in shifts.

Three products. One workflow.

Human in the loop to full autonomy - via an audited, controlled, scalable total solution.

1 DeepTempo

DETECT

LogLM, a foundation model for system telemetry. Sees recon, lateral movement, C2, and exfil. **Zero-shot,** no signatures, no per-environment retraining.

2 vStrike

FUSE

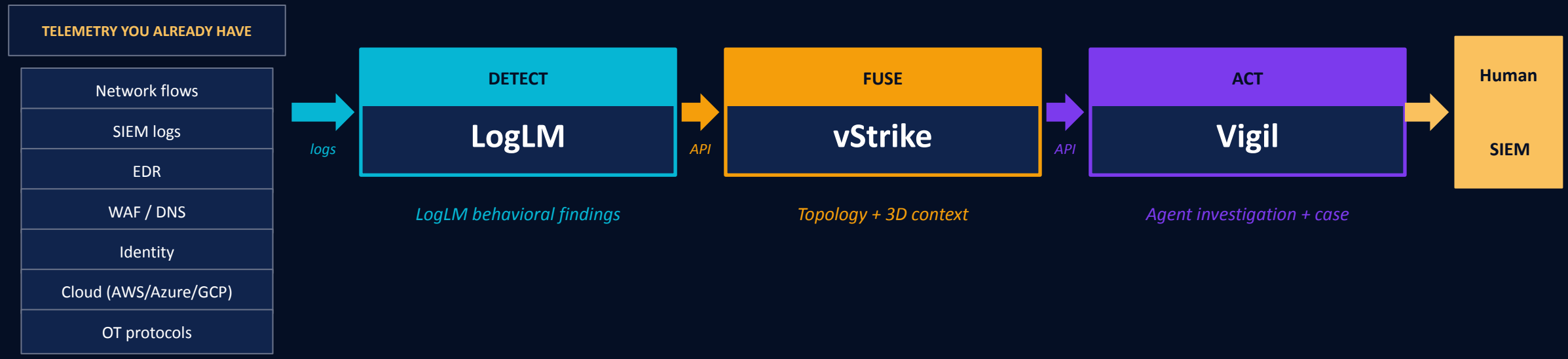
CloudCurrent's fusion layer. Drops every alert onto a live 3D operational picture of IT, OT, IoT, and cloud. Speaks Netflow, Modbus, DNP3, IEC 61850, BACnet.

3 Vigil

ACT

Open-source AI SOC, Apache 2.0. A coordinated team of agents triages, investigates, contains, and writes the case. Open MCP integrations.

How the stack fits together



PRINCIPLES THAT HOLD ACROSS THE STACK

Open standards

MCP for tools, standard APIs and log forwarders for data.

Your data, your env

Cloud, tenant, on-prem, or air-gapped flyaway kit.

No rip-and-replace

Layers onto the SIEM, EDR, and OT tools you already own.

Reversible by design

Every agent action is logged and can be undone.

What customers are seeing

95%+

Reduction in false-positive alert fatigue

10×

Faster mean time to detect

<1%

False positive and false negative rate

<1hr

Time to value from deployment

Source: DeepTempo customer deployments and enterprise case studies.

vStrike: the live operational picture

Every detection lands on a real asset, in a real location, on a real network path.

Single live view of the whole environment

IT, OT, IoT, and cloud rendered in 3D as one operational map.

Grounds every alert in topology

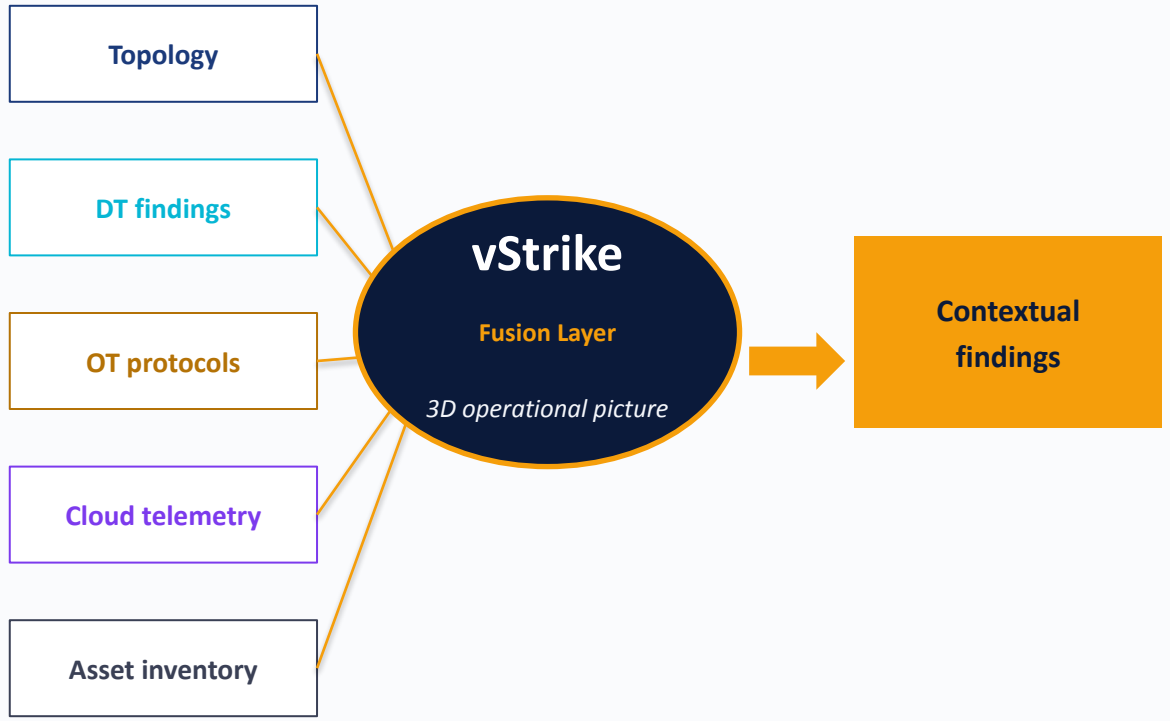
Asset, segment, mission system, and adversary pathway are visible before anyone acts.

Auto-discovers assets others miss

Rogue PLCs, lost workstations, and shadow segments come into view.

Replays incidents as a 3D timeline

Step through what happened, when, and where on the network.



DETECT

DeepTempo LogLM

*Finding the **patterns of life** that traditional solutions miss - without the overhead of traditional Machine Learning*

Behavioral findings, zero-shot

Recon, lateral movement, C2, and exfil, surfaced from raw telemetry.

Trained on security data only

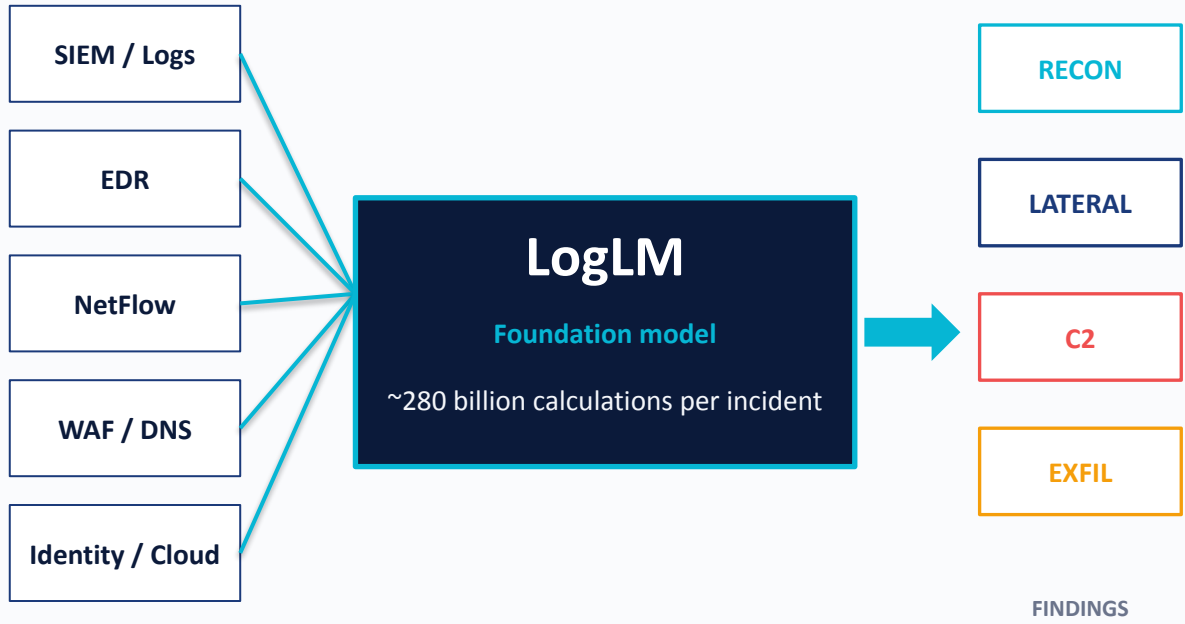
A vertical model. Not a generative LLM bolted on top of logs.

Layers onto existing telemetry

SIEM, EDR, NetFlow, WAF, DNS, identity, cloud. No new agents.

MITRE ATT&CK on every finding

Each alert ships with the technique chain and a behavioral score.



Zero-shot inference. No signatures. No per-environment retraining.

Vigil: open-source AI SOC

A team of specialized agents triages, investigates, contains, and writes the case.

7,200+ detection rules

Sigma, Splunk, Elastic, KQL indexed

30+ integrations

Splunk, CrowdStrike, MISP, Jira…

MCP-native, multi-LLM

Claude, OpenAI, or local Ollama

Markdown playbooks

Edit a file. No DSL. No GUI builder.

The IT/OT seam is one place that attackers hide

vStrike reads OT protocols natively. The operational map covers segments other tools miss.

Modbus	DNP3	IEC 61850	BACnet
Industrial controllers, energy, manufacturing	Power generation and transmission, water utilities	Substations and grid automation	Building automation, HVAC, facilities

WHAT THIS MEANS ON THE GROUND

Surfaces assets other tools miss. Rogue PLCs, lost workstations, shadow OT segments, and cross-domain attack paths across IT, OT, and cloud in one 3D view.

ONE EVENT, START TO FINISH

Example: an OT jump host goes off-script

No existing rule fires. Here is what the stack does.

1 DeepTempo

WHAT HAPPENS

The jump host starts talking to systems it has never talked to. LogLM flags credential-access behavior and tags the MITRE chain.

WHAT YOU SEE

A behavioral score and what is different from this host's normal.

2 vStrike

WHAT HAPPENS

vStrike drops the finding onto the 3D operational map. The affected asset lights up. Adjacent OT segments and reachable hosts come into view.

WHAT YOU SEE

A replay of the incident with the impacted gear highlighted.

3 Vigil

WHAT HAPPENS

From inside vStrike, an analyst kicks off Vigil's Incident Response playbook.

WHAT YOU SEE

A case file with reasoning, evidence, and a recommended fix.

4 You

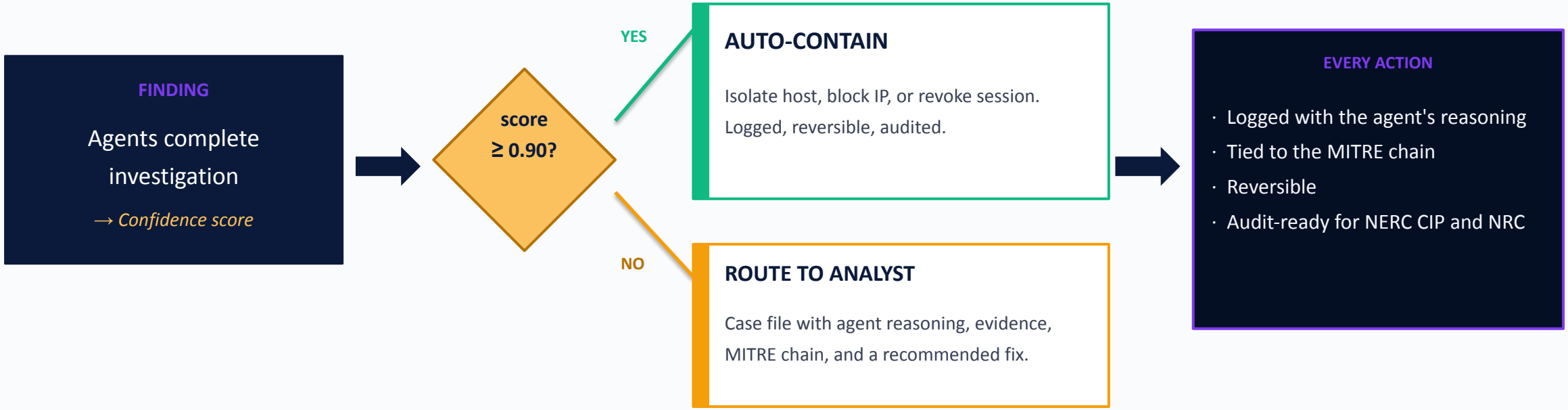
WHAT HAPPENS

Vigil contains autonomously above the confidence threshold. Otherwise it stops and asks. Every action is logged and reversible.

WHAT YOU SEE

An approval trail. NERC CIP and NRC paperwork in hours.

Your Journey to Autonomy - simplified



WHY IT WORKS FOR REGULATED ENVIRONMENTS

Compliance paperwork goes from days to hours. The agents keep the receipts. The analyst keeps the keys.

WHY IT FITS DoW / DISA

A deployable stack, from the future - available today.

Journey towards AI-powered autonomy with control and visibility.

ZERO-SHOT, NO RETRAINING

LogLM brings behavioral detection on day one. No per-environment model tuning to stand up a deployment.

OPERATIONAL CONTEXT, BY DEFAULT

vStrike grounds every finding in topology, segments, and mission systems. Detections become actionable.

OPEN SOURCE, INSPECTABLE

Vigil is Apache 2.0. Read the agents, audit the playbooks, change them in a text editor. No lock-in.

AIR-GAPPED AND FLYAWAY-READY

Runs in your tenant, in your data center, or in a flyaway kit cleared for DOE, IC, and DoD environments.

THANK YOU · QUESTIONS WELCOME · SEE THE SYSTEM LIVE AT THE TAC: https://thetac.tech/

EVAN POWELL
DeepTempo · deeptempo.ai

AARON BOTELER
CloudCurrent · cloudcurrent.biz

VIGIL · OPEN SOURCE
vigilsoc.org · github.com/Vigil-SOC

09 · LIVE DEMO

From raw flow logs to an approved containment.

Running against a simulated hybrid IT/OT/cloud network built for this talk.

PART 1 · DETECT

Evan

Flow logs ingested. DeepTempo returns behavioral findings, zero-shot.

PART 2 · FUSE

Aaron

Findings flow into vStrike. Enriched, contextual output in 3D.

PART 3 · ACT

Evan

Vigil runs the case: timeline, MITRE chain, audit-ready output.