



CASE STUDY | PREPARED BRIEFING COPY | 14 SEPTEMBER 2026

From OT Telemetry to Operator-Ready Evidence

DeepTempo's Intelligent Defense Platform identified an OT attack inside TAC's water-plant range with no signatures and no per-environment training.

EVALUATION CYCLE July – August 2026 ARTIFACTS VERIFIED August 2026 PUBLISHED 14 September 2026

CUSTOMER	ENVIRONMENT	DEPLOYMENT	PLATFORM	HARDWARE
Technology Advancement Center	WS3 water-plant range	Passive, on-premises Finalized-PCAP batch	LogLM + Vigil Intelligent Defense Platform	NVIDIA Jetson AGX Orin

RESULTS

Behavior-based OT detection, inside TAC's local environment.

LogLM ran pretrained against TAC's own OT telemetry with no site-specific tuning, and read the intent behind the traffic rather than flagging outliers. Vigil, the leading open source AI SOC, then gave analysts the underlying protocol activity behind every finding.

Rogue HMI-01

Rogue HMI-01 activity surfaced without a TAC-specific rule

40,773

Canonical flows in WS3 water-plant data

489

Persisted findings in Vigil across four TAC datasets

CHALLENGE

Turning raw OT traffic into usable evidence

DEPLOYMENT FOOTPRINT | This case study focuses on TAC's WS3 water-plant validation. Other TAC environments are outside the validation claims documented here.

- Turn traffic into context.** Raw packet data has limited investigative value unless network flows are enriched with semantic protocol behavior, including Modbus reads and writes.
- Protect plant operations.** Monitoring needed to remain passive and operate without direct participation in the control loop.
- Respect local custody.** Processing and review needed to run within TAC's infrastructure and data-custody requirements.
- Make findings usable.** Analysts needed a way to inspect the evidence behind an anomaly, not just receive an unexplained alert.

ONSITE APPROACH

From finalized PCAP to operator-ready investigation

Finalized packet captures were processed on the NVIDIA Jetson AGX Orin through flow preparation, semantic Modbus extraction, and one-shot LogLM inference. Accepted result bundles were then imported into Vigil for analyst review.

01	02	03	04	05
CAPTURE	PREPARE	DETECT	ACCEPT	INVESTIGATE
Finalized PCAP	Flows + Modbus	Local LogLM	Verified bundle	Vigil evidence

- Passive collection.** The workflow observed traffic without issuing commands to the plant or altering control behavior.
- Intent-aware detection.** LogLM read the behavior of each sequence and judged intent against pretrained OT patterns, rather than scoring outliers against a threshold.
- Protocol-level evidence.** Vigil presented behavioral findings alongside the associated network flows and Modbus operations.
- Fail-closed handoff.** Only accepted result bundles were made available for analyst review.

Deployment boundary. The platform runs in batch or as a continuous stream. The onsite implementation processed finalized PCAPs in batches; it did not include continuous real-time inference or direct SCADA control-loop integration.

VALIDATION SPOTLIGHT

Rogue HMI-01: behavior-based discovery

Pretrained and unadapted, with no TAC-specific signature, device rule, or fine-tuning for the endpoint, LogLM read the sequences involving Rogue HMI-01 as adversarial behavior on first pass. Vigil then exposed the associated network flows and Modbus operations—including register reads and writes—for protocol-level investigation.

TAC's range supplied the separate scenario context: Rogue HMI-01 represented the rogue HMI, and its competing commands caused the simulated flow valve to fluctuate against commands from the benign HMI.

Rogue HMI-01 ANOMALOUS SEQUENCE SURFACED	98.95% MODEL CONFIDENCE	150 MODBUS OBSERVATIONS 120 READS / 30 WRITES
--	---	--

- Detection.

LogLM identified the intent behind the sequences involving Rogue HMI-01, at 98.95% confidence, on a first unadapted run.
- Investigation evidence.

Vigil exposed the corresponding flow and Modbus activity for analyst review.
- Scenario ground truth.

TAC's range scenario identified Rogue HMI-01 as the rogue HMI and linked its competing commands to the simulated process effect.

Here, "out of the box" means that no TAC-specific signature, endpoint rule, or model fine-tuning was added for Rogue HMI-01; standard deployment and pipeline configuration were still required. Model confidence describes confidence in the anomaly verdict, not an attack-probability score.

VALIDATION DATA

Proof from accepted onsite runs

The accepted WS3 water-plant validation artifacts showed repeatable processing from packet capture through findings import, with semantic Modbus evidence preserved for investigation. Results below are specific to the named accepted artifacts, not general production guarantees.

VALIDATION SET	METRIC	ACCEPTED RESULT
WS3	Canonical flows	40,773
WS3	Modbus observations	4,149
WS3	Complete Modbus observations	4,143
WS3	Semantic Modbus events	8,295
WS3	Behavioral findings	287
WS3	Parser warnings / malformed records	0 / 0
WS3	Independent-run semantic comparison	Identical
Attended capture	Canonical flows	628
Attended capture	Modbus observations	268
Attended capture	Behavioral sequences	43
Attended capture	Findings imported into Vigil	43

- Repeatable.** Two independent runs of the WS3 water-plant data produced semantically identical accepted results.
- Fail-closed.** The handoff required bundle acceptance before findings were made available in Vigil.
- Inspectable.** Network and Modbus evidence remained available for investigation rather than being reduced to an opaque alert.
- Passive.** The workflow observed plant communications without issuing control commands.

IMPACT

From behavioral detection to protocol evidence

Vigil, the leading open source AI SOC, gave TAC analysts a direct path from a LogLM behavioral finding to the underlying OT protocol activity. Modbus reads and writes became first-class investigation evidence alongside ordinary network telemetry.

The Rogue HMI-01 result is the clearest example: the workflow surfaced behavior associated with the endpoint identified as the rogue HMI in TAC's range scenario, without depending on a device-specific detection rule. TAC separately supplied the scenario ground truth and simulated process effect.

OBSERVED VALIDATION SNAPSHOT

A read-only audit found 489 persisted findings across four TAC datasets, 6 conversations, 16 chat messages, and 10 LLM interaction records.

CUSTOMER PERSPECTIVE

A joint operational validation

Following the onsite implementation, TAC supplied an attributed perspective on the value of plant-aware analysis and prospective protocol coverage. The engagement is best understood as a joint operational validation: TAC contributed the range, scenario context, and analyst perspective; DeepTempo contributed the Intelligent Defense Platform: LogLM behavioral detection and the Vigil investigation workflow.

TAC PERSPECTIVE

"DeepTempo.ai is providing a powerful analyst assistant capability that adds true plant-operating-state semantic analysis, joining its established IT analysis with meaningful, plant-aware OT analysis. Initially focused on ModbusTCP monitoring and control traffic, near future coverage will expand to include DNP3, EthernetIP, and other ICS protocols, providing significant coverage for SOC monitoring of critical infrastructure plant operations"

— Steve Hutchinson, Director of Research, Technology Advancement Center (TAC)

NEXT STEPS

Building upon the foundation

The onsite work established a foundation for several capabilities:

Intent-weighted comparison. LogLM measures live telemetry against patterns it already carries, judging which departures signal adversarial intent rather than ordinary variation.

Streaming in the plant. The platform runs in batch or as a continuous stream; extending the finalized-PCAP OT workflow to continuous plant telemetry is the next step onsite.

Plant-state representation, estimation and tracking. Model design conditions, operating modes, recipe setpoints, and production timing can provide additional context as a desired-state reference.

Causation support (multi hypothesis/likelihood scoring). Workflows to automate the analysis of divergence and protocol evidence in Vigil, to accelerate the determination of likely causes, severity, and courses of action.

About the partners

Technology Advancement Center

TAC is a nonprofit focused on creating and propelling enduring technological advantages for the nation through workforce development, proof-of-concept innovation, and collaboration.



DeepTempo

DeepTempo builds the Intelligent Defense Platform for cybersecurity: LogLM, a purpose-built foundation model that identifies attacker intent directly from telemetry without relying on signatures or brittle rules, and Vigil, the leading open source AI SOC. Both run inside the customer's boundary, on their infrastructure, with their models and their workflows.

www.deeptempo.ai