DeepTempo

# Case Study

## Advancing Operational Technology Security with AI-Powered Threat Detection

**DeepTempo Partnership with
CloudCurrent and the Technology Advancement Center (TAC)**

### Executive Summary

DeepTempo partnered with CloudCurrent and the Technology Advancement Center (TAC) to demonstrate the capabilities of LogLM, our AI-powered security foundation model, in monitoring and protecting operational technology (OT) environments. Working alongside CloudCurrent’s VStrike Platform, this collaboration showcased high-accuracy threat detection with minimal false positives and false negatives in complex industrial control system networks.

The engagement validated DeepTempo's ability to process industrial network traffic, identify sophisticated attack patterns, and provide actionable intelligence through seamless integration with this advanced visualization platform. Results demonstrated clear differentiation between benign operational traffic and malicious activity, with MITRE ATT&CK classification enabling operators to understand and respond to threats effectively.

### The Growing Threat to Critical Infrastructure

Recent years have seen a dramatic increase in cyberattacks targeting operational technology environments that control critical infrastructure. High-profile incidents have demonstrated the real-world consequences of inadequate OT security and brought national attention to the vulnerabilities in industrial control systems.

The Colonial Pipeline attack in May 2021 disrupted fuel supplies across the Eastern United States, causing widespread shortages and demonstrating how cyberattacks on industrial systems can have immediate, tangible impacts on daily life. The attack led to a state of emergency declaration in multiple states and highlighted the interconnection between IT and OT systems in critical infrastructure.

# About the Partners

Similarly, the 2021 incident at the Oldsmar, Florida water treatment facility raised alarms when an intruder accessed the plant's control systems and attempted to modify chemical treatment levels to dangerous concentrations. While the attack was detected and remediated before any harm occurred, the incident underscored the vulnerability of municipal water systems and other critical infrastructure to cyber threats. These events have driven increased investment in OT security and highlighted the need for AI-powered detection capabilities that can identify threats in complex industrial environments.

## Technology Advancement Center (TAC)

The Technology Advancement Center (TAC) is a non-profit organization dedicated to creating and propelling enduring technological advantages for the nation. Operating out of TheLink, a dynamic 72,000-square-foot facility in Columbia, Maryland, TAC serves as a collaborative space where the technology and cybersecurity community can connect, innovate, and advance defense capabilities.

TAC operates sophisticated OT ranges that simulate real-world critical infrastructure environments, including manufacturing facilities, municipal water systems, and power grid operations. Their mission encompasses academic engagement, proof-of-concept innovation, workforce development, and small business engagement. TAC's facilities serve as proving grounds for emerging security technologies and training environments for the next generation of OT cybersecurity professionals, having trained thousands of professionals and engaged tens of thousands of students.

## CloudCurrent and VStrike

CloudCurrent develops VStrike, an advanced visibility and security operations platform built for the realities of complex IT, OT, and cloud environments. It delivers real-time network mapping, event storylining, and full forensic replay, giving operators a clear understanding of the complete context behind activity across their industrial networks.

By ingesting and correlating data from multiple security and operational sensors, VStrike creates a unified operational picture that cuts through noise and fragmentation. Its visualization capabilities transform raw telemetry into clear, actionable insights, enabling teams to detect, investigate, and respond to threats with confidence and precision.

# The Challenge

## The Challenge:

Operational technology environments present unique security challenges that traditional IT-focused solutions struggle to address. Industrial control systems operate with specialized protocols like Modbus that lack the standardized flow records available in IT networks. Additionally, OT environments require continuous monitoring with extremely low tolerance for false positives, which can disrupt critical operations, and false negatives, which can allow attacks to progress undetected.

TAC sought a solution capable of:

- Processing raw PCAP data from OT networks using Modbus and other industrial protocols
- Detecting sophisticated attack patterns including unauthorized access, reconnaissance, and command injection
- Providing high-confidence threat classifications with minimal false positives and negatives
- Integrating with visualization tools for operator-friendly presentation of security intelligence
- Enabling replay and forensic analysis of security events
- Supporting flexible deployment models appropriate for secure environments

## The Solution: DeepTempo LogLM Integration

DeepTempo deployed LogLM, our foundation model for network security, to process PCAP captures from TAC's OT range. The system converts raw packet captures into network flow sequences, processes them through our pre-trained encoder model, and generates threat assessments with MITRE ATT&CK classifications.

LogLM's embedded world model approach enables it to understand the semantic meaning of network traffic patterns rather than relying solely on signature matching. This allows detection of previously unseen attack variants and reduces false positives by understanding the context of network communications within the operational environment.

# The Solution

## Flexible Deployment Options:

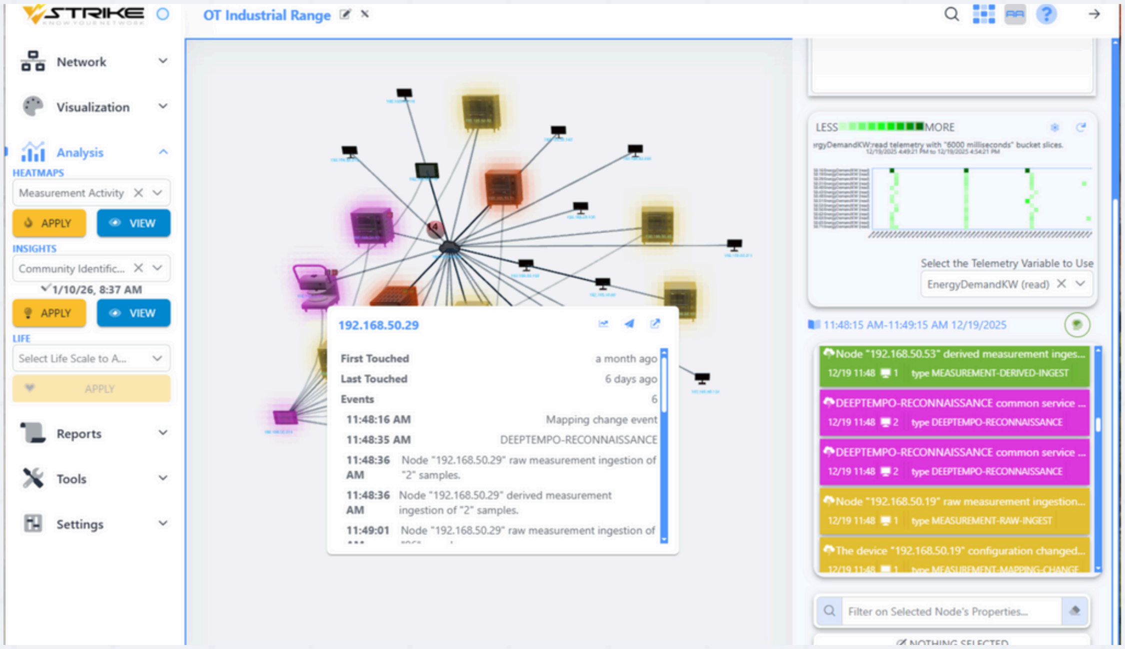
The engagement demonstrated DeepTempo's ability to support multiple deployment architectures. We validated both on-premise deployment options for air-gapped and highly secure environments, as well as secure integration with our cloud-hosted SaaS solution for organizations that prefer managed services.

For many OT environments, particularly those in critical infrastructure sectors, on-premise deployment is the preferred approach. These environments often have strict data residency requirements, air-gapped networks, or regulatory constraints that preclude cloud-based analysis. DeepTempo's architecture supports these requirements while delivering the same high-accuracy threat detection capabilities available in our SaaS offering.

## VStrike Visualization Integration:

DeepTempo's event output was integrated into CloudCurrent's VStrike platform, allowing operators to see threat detections directly within the context of their network topology. The integration adds storyline capabilities that align DeepTempo events with OT telemetry and operational data, giving teams a complete, contextual view of network activity.

VStrike's 3D network mapping automatically highlights affected endpoints when threats are detected, and its replay feature lets operators step through events to understand how an attack unfolded. Together, DeepTempo's AI-driven detection and VStrike's intuitive visualization provide operators with the clarity and confidence needed to respond effectively in complex OT environments.



Community Identific... ✓1/10/26, 8:37 AM

192.168.50.29

| | |
|---|---|
| First Touched | a month ago |
| Last Touched | 6 days ago |
| Events | 6 |
| 11:48:16 AM | Mapping change event |
| 11:48:35 AM | DEEPTEMPO-RECONNAISSANCE |
| 11:48:36 AM | Node "192.168.50.29" raw measurement ingestion of "2" samples. |
| 11:48:36 AM | Node "192.168.50.29" derived measurement ingestion of "2" samples. |
| 11:49:01 | Node "192.168.50.29" raw measurement ingestion of |

rgyDemandKW:read telemetry with "6000 milliseconds" bucket slices.
12/19/2025 4:49:21 PM to 12/19/2025 4:54:21 PM

Select the Telemetry Variable to Use: EnergyDemandKW (read)

11:48:15 AM-11:49:15 AM 12/19/2025

- Node "192.168.50.53" derived measurement inges... 12/19 11:48 1 type MEASUREMENT-DERIVED-INGEST
- DEEPTEMPO-RECONNAISSANCE common service ... 12/19 11:48 2 type DEEPTEMPO-RECONNAISSANCE
- DEEPTEMPO-RECONNAISSANCE common service ... 12/19 11:48 2 type DEEPTEMPO-RECONNAISSANCE
- Node "192.168.50.19" raw measurement ingestion... 12/19 11:48 1 type MEASUREMENT-RAW-INGEST
- The device "192.168.50.19" configuration changed... 12/19 11:48 1 type MEASUREMENT-MAPPING-CHANGE

# Results:

## High-Accuracy Threat Detection

In controlled testing scenarios, DeepTempo successfully identified attack patterns with high confidence and minimal false positives. Analysis of PCAP data containing both normal operations and simulated attacks demonstrated clear separation between benign and malicious traffic patterns.

## Operational Visualization

The integration with VStrike enabled operators to see DeepTempo events synchronized with OT telemetry data, creating storylines that brought security events and operational data together in a common picture. This capability allows defenders to correlate network-based threats with physical process impacts, such as unauthorized register modifications that caused operational faults.

Operators demonstrated the ability to replay security events, step through attack sequences, and understand the full context of threats within their industrial environment. The platform's on-demand forensics capability enables rapid investigation and documentation of security incidents.

## Embedding Space Analysis

Analysis of LogLM's internal representations revealed distinct separation between operational traffic and malicious intent patterns. The model learns to identify attacker intent, reconnaissance, command injection, unauthorized access, rather than statistical anomalies. This separation demonstrates LogLM's ability to detect attacker objectives from structured network sequences, even in the constrained data environment of a test range.

The visualization of embedding space provides explainable evidence of the model's detection capabilities.

## Key Capabilities Demonstrated

- OT Protocol Support: Successfully processed
- Modbus traffic and other industrial protocols common in manufacturing and critical infrastructure environments
- Attack Pattern Recognition: Detected reconnaissance, unauthorized access, and command injection attacks with MITRE ATT&CK classification
- Low False Positive/Negative Rates: Clear separation between benign and malicious traffic enables confident alerting without operational disruption
- Visualization Integration: Seamless event synchronization with VStrike enables operators to understand threats in operational context
- Forensic Replay: Combined solution enables step-through analysis of security events for incident response and training
- Flexible Deployment: Support for both on-premise deployment in secure environments and cloud-hosted SaaS integration

# Results Continued

| Metric | Result |
|---|---|
| Attack Pattern Detection | Successfully identified all simulated attacks |
| MITRE ATT&CK Classification | Reconnaissance (83%) and Command & Control (17%) |
| False Positive Rate | Minimal - clear separation in embedding space |
| Visualization Integration | Seamless sync with VStrike storylines |

## Future Directions:

Building on this successful engagement, DeepTempo and TAC are expanding their collaboration to additional critical infrastructure domains. Planned deployments include municipal water system monitoring, with power grid and healthcare facility environments to follow. These expansions will further validate LogLM's capabilities across diverse OT environments.

The partnership continues to develop automated workflows for PCAP ingestion and analysis, enabling continuous monitoring of TAC's training ranges. This ongoing collaboration advances both security research and the practical deployment of AI-powered threat detection in operational technology environments.

# Next Steps

## Conclusion:

The DeepTempo and TAC partnership, in collaboration with CloudCurrent's VStrike platform, demonstrates the viability of AI-powered security for operational technology environments. By combining LogLM's foundation model approach with advanced visualization capabilities, the solution delivers high-accuracy threat detection with the operational clarity that industrial environments require.

As critical infrastructure faces increasingly sophisticated cyber threats—from nation-state actors to ransomware operators—the need for advanced detection capabilities has never been greater. This engagement validates DeepTempo's approach to network security: using pre-trained models that understand the semantic meaning of network traffic to detect sophisticated threats while minimizing false positives. The combination of AI-powered detection, intuitive visualization, and flexible deployment options provides defenders with the tools they need to protect essential systems.

## About DeepTempo

We're building the collective defense platform necessary to defend our businesses and critical infrastructure from the new breed of adversaries armed with the power of AI and the cloud. Together, we shall reclaim the advantage.

DeepTempo: The AI for Threat Detection.

Learn more: https://www.deeptempo.ai/

Follow us on LinkedIn:_ https://www.linkedin.com/company/deeptempo/