DeepTempo

Tempo
A Transformer-Based Log Language Model for Advanced Cybersecurity Defense

DeepTempo

April 2025
deeptempo.ai

Executive Summary

Cybersecurity attacks are more sophisticated than ever; attackers are more professional and productive, leveraging LLMs to rapidly develop and evolve attacks. McKinsey and Company projects total losses of approximately $10.5 trillion from cyber attacks in 2025. Traditional rule-based and legacy machine-learning solutions have failed to keep pace and are unable to see advanced attacks and attacks that have been morphed with the help of LLMs; these systems also burden security operations centers (SOCs) with high false-positive rates and escalating costs and a sprawl of point products.

Tempo, developed by DeepTempo, is a first of its kind Foundation model for cybersecurity. Tempo is a transformer-based Log Language Model (LogLM) leveraging state-of-the-art deep learning and self-attention mechanisms to deliver highly accurate, adaptable, and context-rich incident identification and isolation. With proven false positive rates of below 1% and rapid adaptability via fine tuning, Tempo provides unparalleled precision. Security Operations Centers (SOCs) benefit from Tempo's alerts, which include detailed context, entity resolution and seamless MITRE ATT&CK mapping. Tempo is also used to rapidly triage attacks, leveraging rapid semantic search to isolate potential attacks that otherwise would not be identified by traditional queries of logs.

Tempo helps reduce security costs by boosting analyst productivity while decreasing costs for SIEM ingestion. Over time, Tempo will remove the need for a range of point products that are built around rule-based indicators, integrations and workflows to detect specific types of attacks, such as data loss prevention and insider threat detection. Lastly, Tempo remains accurate over time thanks to active learning.

Tempo is available today on the Snowflake marketplace as the only NativeApp for security incident identification and can be deployed on premise or any cloud environment with access to historic and near real time logs.

Why Tempo: Transformative Cybersecurity Defense

Tempo leverages foundational deep learning principles previously used in large language models (LLMs) and in particular encoder-only deep learning models. However, Tempo is pretrained and tuned for cybersecurity logs and event data, resulting in the following significant advantages:

1

Improved Detection of Advanced and Evolving Threats

Traditional cybersecurity tools depend heavily on signature-based rules or supervised ML, both limited in recognizing novel and evolving threats. Tempo employs a transformer architecture that learns deep contextual relationships in log sequences, allowing it to detect subtle and previously unseen anomalies.

- **Self-supervised Learning:** Tempo's self-supervised approach learns directly from unlabeled data, significantly improving detection accuracy for novel threats without the delays and biases introduced by manual labeling.
- **Long-Range Dependency Modeling:** Unlike earlier models, Tempo leverages self-attention to effectively capture and interpret long-range relationships within log sequences. This assists both in the identification of more complex attacks and also helps to reduce false positive rates.

2

Rapid Scope Analysis of Potential Attacks

Once an anomaly is identified, Tempo provides SOC analysts with immediate contextual insights:

- **MITRE ATT&CK Mapping:** Tempo automatically aligns anomalies with relevant MITRE ATT&CK patterns via the use of a tuned classifier, accelerating incident analysis and response.
- **Entity Resolution:** Again using a tuned classifier, Tempo learns the types of entities that are present in a network, information from log data, rapidly pinpointing affected users, hosts, and other devices, essential for analysts working to quickly contain threats.
- **Semantic Search - Forensichat:** An optional capability is the use of a natural language based interface to quickly perform sequence based searches; this utility identifies similar patterns to concerning sequences, whether MITRE ATT&CK or other identified sequences.

This immediate context is invaluable for proactive threat hunting, incident triage, and forensic investigation, greatly enhancing analysts' productivity and effectiveness.

3

Cost Savings through Enhanced Accuracy and Efficiency

Tempo's advanced modeling and filtering capabilities lead directly to significant operational cost savings:

- **Lower False Positives (1-5%):** With precision rates consistently exceeding traditional methods, Tempo drastically reduces false-positive alerts, directly mitigating SOC burnout and freeing analysts to focus on genuine threats. The false positive rate depends on the distribution of the underlying data vs. the distributions upon which Tempo has been trained; the active learning system of Tempo helps to adapt the model and related software to new environments.
- **Reduced SIEM Ingestion Costs:** Tempo efficiently identifies and forwards only high-fidelity indicators to SIEM systems, substantially cutting the costs associated with processing and storing raw log data.
- **Simplification:** Tempo often replaces dozens of hard to maintain rules and ML models. With attacks becoming more advanced and novel, existing rules and ML models are more frequently ineffective, requiring increased maintenance. In contrast, Tempo sees novel attacks quickly, without any additional adaptation.

Key Capabilities of Tempo

→

Foundation Model Advantage: Rapid Generalization and Flexibility

Tempo's transformer-based architecture provides rapid and robust generalization across cybersecurity environments. Unlike traditional ML models that require extensive retraining for each new context, Tempo generalizes quickly from initial pre-training and can be fine-tuned efficiently for specific environments, dramatically shortening the time to operational value.

→

Self-Supervised Training for Enhanced Accuracy

By training solely on benign data through a self-supervised approach, Tempo effectively understands normal behavior, enabling accurate detection of previously unseen anomalies. This method avoids the limitations and biases inherent in label-based training.

→

Context-Rich Detection through Semantic Embeddings

Tempo creates semantic embeddings from logs, capturing complex contextual information. These embeddings:

- Map to the MITRE ATT&CK framework, offering SOC analysts quick, actionable insights into attacker tactics
- Support entity resolution, clarifying identities involved in incidents, and accelerating investigation workflowsEnable powerful semantic search capabilities, further enriching threat hunting and forensic investigations

→

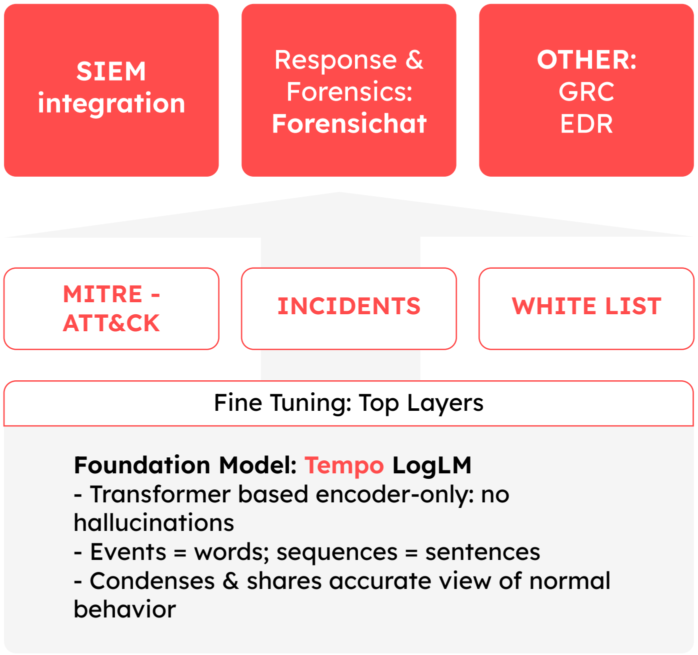
Active Learning and Self-Calibration

Cybersecurity environments evolve continuously; Tempo's built-in patent pending active learning mechanisms ensure it keeps pace. By continuously embedding and identifying potential data drift, Tempo self-calibrates over time, constantly refining its accuracy and adaptability without costly manual interventions.

Technical Implementation: How Tempo Works

Tempo’s innovative approach integrates several key components:

- **Transformer Architecture:** Using a multi-layer, multi-head self-attention mechanism, Tempo effectively captures long-range and subtle relationships within log data, essential for recognizing advanced threats.
- **Multi-layer architecture with a Foundation Model and Classifiers:** As a foundation model, Tempo is built to support downstream tasks such as MITRE ATT&CK and threat intelligence classification. Additionally this architecture supports rapid fine tuning to novel environments.
- **Active learning:** The adaptability of Tempo and its ability to adapt quickly to new domains enable a self learning capability called Active Learning which reduces by 75% or more the time necessary to maintain and tune Tempo versus the care and feeding of traditional ML systems.



SIEM integration

Response & Forensics: **Forensichat**

OTHER: GRC EDR

MITRE - ATT&CK

INCIDENTS

WHITE LIST

Fine Tuning: Top Layers

Foundation Model: Tempo LogLM
- Transformer based encoder-only: no hallucinations
- Events = words; sequences = sentences
- Condenses & shares accurate view of normal behavior

User Interfaces
- SIEM: more accurate & context
- Forensichat: threat response
- Future: all incident identification

Northbound integration
- Feeds into SIEMs
- Forensichat UX

Classifiers
- Use underlying embeddings
- Efficient to fine tune & adapt

Fine Tuning - Foundation Model
- No labels needed

Foundation Model
- Learns from diverse datasets
- Collective Defense
- Generalizes quickly

Deploying Tempo: Immediate Impact and Long-Term Value

Tempo integrates seamlessly into existing cybersecurity architectures, either near log sources or as part of larger security data lakes, feeding actionable intelligence downstream to SIEMs or SOAR platforms.

Immediate benefits include:

- Rapid incident identification with high accuracy.
- Immediate availability of threat context such as MITRE ATT&CK mappings and entity resolution.
- Simplification of operations by replacing dozens or hundreds of ineffective rules and ML models with the self adapting Tempo.

Tempo evolves continuously through active learning, refining its detection capabilities without manual retraining costs, making it a sustainable and strategic cybersecurity investment.

Conclusion:
The Tempo Advantage

In the face of ever-escalating cyber threats and operational demands, Tempo represents a step forward in cybersecurity defense. By combining the power of transformer-based foundation models with self-supervised learning and active adaptation, Tempo provides:

- Unmatched detection of sophisticated and evolving threats
- Immediate, actionable incident context
- Significant operational cost savings through reduced false positives and SIEM ingestion costs

DeepTempo's Tempo LogLM is a strategic shift, enabling cybersecurity teams to proactively identify, understand, and respond to cyber threats with unprecedented accuracy, efficiency, and resilience.

For more information or to schedule a demonstration, visit www.deeptempo.ai

DeepTempo