MixMode®

Countering Adversaries Leveraging Frontier-Level AI Attacks

Machine-Speed Novel Threat Detection Powered by Self-Learning, Self-Supervised AI

The threat calculus has changed. Mythos-class foundation models and unrestricted open-weight alternatives have given adversaries offensive capabilities far beyond what human operators alone could previously achieve. MixMode AI detects what these systems produce—novel, never-before-seen attacks—in real time, at scale, even in disconnected, disconnected, degraded, intermittent, and limited (DDIL) environments.

The Frontier-AI Threat

- Per-Target Malware: Tooling and phishing infrastructure regenerate per target, per hour—nothing for signatures to match.
- Machine-Speed Campaigns: Recon to exfiltration compressed from months to minutes.
- Patient Automation: Low-and-slow operations using legitimate credentials and native tooling—no malicious artifacts to flag.
- Deliberate Noise: AI-generated alert floods engineered to bury the real intrusion inside rule-based SIEMs.

The MixMode Answer

- Self-Supervised AI: Learns each environment without rules, signatures, or historical training data.
- Behavioral Forecasting: Continuously forecasts expected operational context and flags deviations—including the telling absence of expected activity.
- No Signature Required: An AI-generated attack must still deviate to act. That deviation is precisely what MixMode detects—no pre-training required.
- Machine-Speed Defense: Real-time, pre-attack indicators with no ML/LLMs, GPUs, or cloud necessary for detection.

Adversaries will bring frontier AI to the fight. MixMode ensures defenders bring better—proprietary, patented AI proven at the US DoW and US Intelligence Community, operating at machine speed wherever the mission requires.

Key Benefits

Detect AI-Generated Attacks: Flag never-before-seen tooling—mutated per target by frontier models—that signature-based systems structurally miss.

Counter Machine-Speed Campaigns: Reduce MTTD and MTTP with real-time, pre-attack indicators against fully automated adversary operations.

Expose Patient AI Agents: Surface low-and-slow, living-off-the-land activity through continuously evolving forecasts of your environment.

Resist Alert Flooding: Deviation-ranked detections cannot be drowned out by adversary-generated noise that overwhelms rule-based SIEMs.

Supply-Chain Resiliency: Hardware agnostic—no ML/LLMs, no GPUs, no cloud. Fully functional in air-gapped and DDIL environments, beyond the reach and risk of frontier-model supply chains.

Accredited: Already accredited and employed by the US DoW and US Intelligence Community.

www.mixmode.ai | +1 (858) 225-2352 | info@mixmode.ai |