DETECT & STOP AI-GENERATED ATTACKS WITH MIXMODE

## Stop AI-Generated Attacks in Real-time with MixMode

As artificial intelligence (AI) continues to advance, there is a growing concern about the emergence of AI-generated attacks. Threat actors are harnessing the power of artificial intelligence to develop sophisticated attack techniques that can evade traditional security measures, making them highly elusive and difficult to detect using conventional methods. These AI-generated attacks have the potential to cause substantial damage to organizations, compromising sensitive data, disrupting operations, and undermining trust.

Detect What Others Can't with MixMode

The MixMode Platform is the only generative AI cybersecurity solution built on patented Third Wave AI for real-time threat detection and response. The Platform seamlessly integrates with any security environment to understand, adapt, and evolve to detect threats in real-time, at scale.

MixMode's patented, self-learning AI was designed to identify and mitigate advanced attacks, including adversarial AI. An adversary would need to have a deep understanding of MixMode's algorithms and processes to evade detection. However, in attempting to learn and replicate MixMode's AI, the adversary's behavior would likely be detected as anomalous by the platform, triggering an alert and preventing any further damage.

NO RULES. NO TUNING. NO DATA LIMITS. ANY ENVIRONMENT.
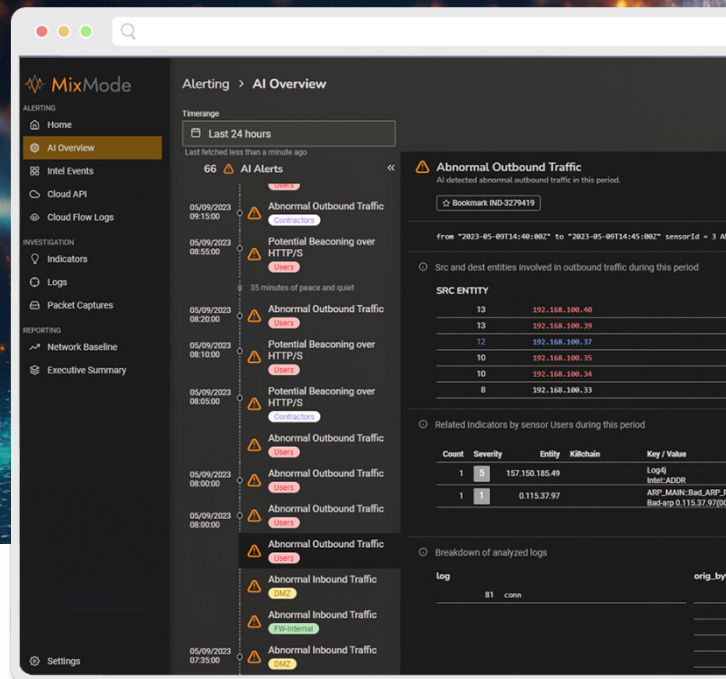
The MixMode Platform is your best defense against AI Generated Attacks, enabling security teams to:

Identify Advanced Threats: Detects and prevents threats that bypass traditional security measures, including AI Generated Attacks, Zero-Day, Insider Threats, New Ransomware, "Living off the Land", Supply Chain, AI/ML Model Poisoning.

Automate Threat Detection: Real-time and predictive dynamic threat detection and response for novel and known attacks at scale for cloud, on-prem or hybrid environments.

Detect in Real-time at Scale: Easily monitor massive volumes of data in real-time to quickly detect and mitigate threats without increasing spend.

Increase Efficiencies: Make informed decisions and save time by focusing on the threats that matter and avoiding false positives that don't.