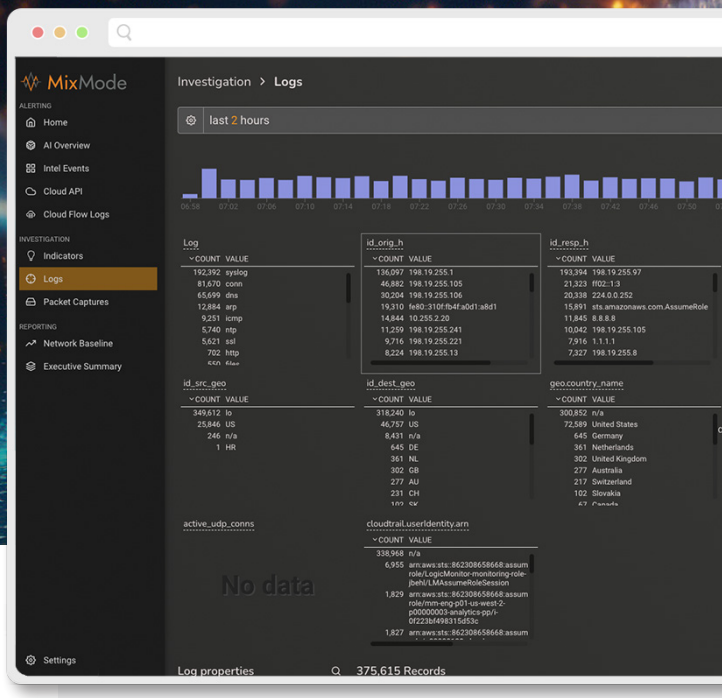
MixMode®

AUTOMATED THREAT HUNTING WITH MIXMODE



Automate Manual Threat Hunting Processes

Traditional threat-hunting methods heavily rely on manual analysis and human intuition, which can be time-consuming, resource-intensive, and prone to human error. Security teams need help to keep pace with the ever-evolving threat landscape and identify sophisticated threats evading traditional security controls. The usual reactive approach leaves organizations vulnerable to undetected threats, resulting in potential data breaches, financial losses, and reputational damage.

Detect and Remediate Threats 99.7% Faster

The MixMode Platform is the only generative AI cybersecurity solution built on patented Third Wave AI for threat detection and response. MixMode's self-learning AI was born out of the dynamical systems branch of mathematics and adapts itself to the specific dynamics of each network, understanding and evolving to identify threats as they arise.

The MixMode Platform includes forensic capabilities with full packet capture and file extraction, enabling security teams to automatically and proactively hunt for malicious events in their environments. This helps automate manual processes and allows threat hunters to focus on investigating and take proactive steps to mitigate risks and prevent future attacks.

The MixMode Platform autonomously analyzes data from various sources to identify patterns, anomalies, and relationships between seemingly unrelated events. This contextual analysis helps uncover hidden patterns and enables threat hunters to trace the attack chain, identify the root cause, and understand the full extent of an attack.

NO RULES. NO TUNING. NO DATA LIMITS. ANY ENVIRONMENT.

MixMode empowers security analysts with the tools they need to:

Automate Detection at Scale: Easily monitor large volumes of data in real-time to quickly detect and mitigate threats across any attack surface without increasing spend.

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

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

Reduce Costs: Reduce storage costs and eliminate the need for multiple disparate toolsets while up-leveling existing investments.