MIXMODE IDENTITY THREAT DETECTION AND RESPONSE

Real-time Threat Detection of Identity Threats at Scale

Identity-driven attacks targeting user credentials are among the most popular techniques cybercriminals use to access enterprise networks. Attackers continuously evolve tactics to evade detection and exploit vulnerabilities, making these attacks highly targeted, customized, and challenging to detect using traditional security measures.

Enterprise organizations have complex identity ecosystems, with the sheer volume and complexity of identity data making it difficult to identify suspicious or abnormal behavior that could indicate a threat.

MixMode's Identity Threat Detection and Response Solution provides real-time monitoring of your identity infrastructure, capable of ingesting and analyzing large volumes of diverse data from multiple systems. MixMode ITDR continuously monitors your environment and correlates behavioral, access, and log data to proactively identify threats targeting credentials, privileges, cloud entitlements, and the systems that manage them.

How it Works

Most cybersecurity solutions utilize First and Second Wave artificial intelligence in various ways. However, these still rely on rules-based systems which can only detect attacks with known signatures and cannot effectively scale to the size of a typical corporate network.

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 result is a truly autonomous defense system that dramatically enhances security programs, detects threats others miss in real-time, and delivers tangible business outcomes in days.

KEY BENEFITS

Real-time Detection

Real-time and predictive dynamic threat detection for novel and known attacks.

Increased Efficiencies

Uplevel existing investments, do more with less and save time by focusing on the threats that matter.

Seamless Integration

No rules, training, onboarding, or tuning required, delivering tangible results in days.

Enhanced Visibility

Contextual dashboards with AI-informed insights and detailed visibility.

Proven Scalability

Easily monitor large volumes of data in real-time to quickly detect and mitigate threats without increasing spend.

STOP WASTING TIME CHASING FALSE POSITIVES AND START FOCUSING ON THE THREATS THAT MATTER.

Real-time Threat Detection: Real-time and predictive dynamic threat detection for novel and known attacks at scale.

Systematized Investigations: Full packet capture with file extraction, deep packet inspection, and the ability to query metadata or full packets.

Guided Response: Remediation recommendations with linked intelligence and the Mitre ATT&CK Framework.

Automated Threat Hunting: Automate hunting queries and proactively hunt for malicious events with full with our User Defined Rules functionality.

"Enterprise cybersecurity teams waste millions of dollars and man-hours every year storing, aggregating, and managing data with traditional SIEM platforms. The solution is to instead leverage unsupervised AI-driven analysis and predictive anomaly detection across multiple streams of data in real-time, at scale with a platform like MixMode."

Ritu Jyoti, VP of AI Research, IDC

KEY CAPABILITIES

Real-Time Monitoring and Alerts

Continuously monitors user activities, access events, and authentication data in real-time.

Anomaly Detection

Helps identify anomalies that may not be apparent based solely on individual user behavior.

Threat Intelligence Integration

Enriches alerts with threat information and the MITRE ATT&CK framework.

User Entity Behavior Analytics (UEBA)

Identifies patterns and trends that may indicate suspicious activities or potential identity threats, even if the individual events seem innocuous in isolation.

NO RULES. NO TUNING. NO MAINTENANCE. ANY ENVIRONMENT.

MixMode is the leader in delivering generative AI cybersecurity solutions at scale. MixMode offers a patented, self-learning Platform designed to detect known and unknown threats in real-time across cloud, hybrid, or on-prem environments. Large enterprises with big data environments, including global entities in financial services, fortune 1K commercial enterprises, critical infrastructure, and government sectors, trust MixMode to protect their most critical assets. Backed by PSG and Entrada Ventures, the company is headquartered in Santa Barbara, CA. Learn more at www.mixmode.ai.