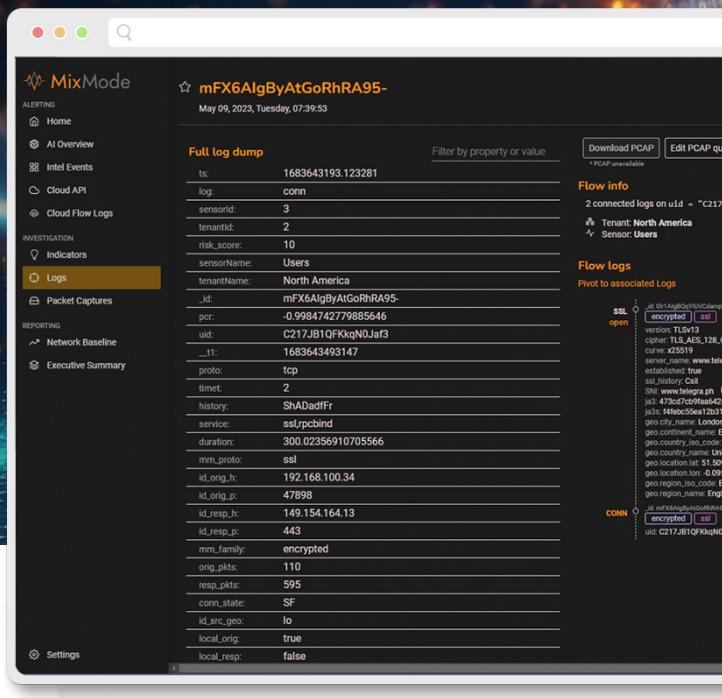
MixMode®

DETECT & PREVENT INSIDER THREATS WITH MIXMODE



Detect Insider Threats in Real-time

Insider threats pose a significant risk to organizations, as malicious or negligent insiders can cause substantial damage to sensitive data, intellectual property, and critical systems. Traditional security measures often focus on external threats, leaving organizations vulnerable to internal threats that are difficult to detect and mitigate. Identifying and addressing insider threats is a significant challenge for security teams, leading to potential breaches, financial losses, and reputational harm.

Automate Detection & Triage to Remediate True Threats 99.7% Faster

The MixMode Platform is the only generative AI cybersecurity solution built on patented technology purpose-built to detect and respond to threats in real-time, at scale, including suspicious behavior that may indicate an insider threat.

The MixMode Platform utilizes self-supervised learning to forecast expected behavior and detect potential threats by analyzing network activity and extracting patterns and trends from the underlying time-stamped data without predefined rules or training.

The MixMore Platform analyzes the behavior and activities of users, systems, and entities within a network or system to identify and surface known or unknown attacks in real-time.

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

The MixMode Platform enables security teams to:

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

Detect ALL Attacks: Detects and prevents threats that bypass traditional security measures, including Insider Threats, “Living off the Land”, Ransomware, Zero-Day, Supply Chain, AI/ML Model Poisoning.

Eliminate Blindspots: Easily monitor and protect the entire attack surface across cloud, on-prem and hybrid environments, to quickly detect and mitigate emerging 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.