MIXMODE CLOUD DETECTION AND RESPONSE FOR AWS

Real-time Threat Detection for VPC Flow Logs and AWS CloudTrail

The cloud has revolutionized how businesses operate, enabling rapid scaling, innovation, and operational agility. However, robust cloud security is crucial as critical functions and sensitive data move to the cloud. Traditional security measures don't fully apply in cloud environments.

The MixMode Platform is a real-time dynamic threat detection and response platform that identifies novel and known attacks at scale for cloud environments. MixMode helps enterprise security teams monitor their AWS network traffic and API calls, including VPC Flow Logs and AWS CloudTrail Logs, in real-time to close gaps in their security posture.

The MixMode Platform is the only generative AI cybersecurity solution built on patented Third Wave AI for threat detection and response. The Platform can be seamlessly installed in minutes, immediately acclimating to autonomously learning, understanding, adapting, and evolving without relying on rules, training, or human interaction. 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 a matter of days.

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.

MixMode's patented self-learning AI platform was born out of the dynamical system's branch of mathematics and identifies patterns and trends without predefined rules or training. MixMode's AI model adapts itself to the specific dynamics of each network, understanding and evolving to identify threats as they arise. The MixMode Platform is the only cybersecurity solution that can predict and surface zero-day attacks in real-time and is proven drastically reduce false positives and deliver 99% alert precision.

KEY BENEFITS

Real-time Detection

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

Unlimited Scalability

Easily monitor large volumes of data within your AWS environment across VPC Flow logs, AWS CloudTrail logs, and on-premise network data.

Unified Visibility

Gain increased visibility into CloudTrail and VPC Flow logs within one platform.

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.

Reduced Costs

Reduce storage costs and eliminate the need for multiple disparate toolsets.

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.

"MixMode starts learning from the first five minutes it is deployed, does not require historical data, and is adapting actively to the dynamic changes in massive amounts of network data."

Ritu Jyoti, VP of AI Research, IDC

KEY CAPABILITIES

Correlate Large Data Sets

Correlate AWS CloudTrail traffic with VPC Flow Logs and/or SIEM logs to identify IPs that cause issues across these data streams.

Increased Insights

Leverage both tools with visibility on a single platform to gain a comprehensive view of your cloud infrastructure.

Compare AWS Data

Compare your CloudTrail and Flow Log traffic against our database(s) of known intel feeds for real-time detection.

Correlate and Search

Correlate data across cloud data to preserve forensic records outside your AWS environment.

NO RULES. NO TUNING. NO DATA LIMITS.

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.