MIXMODE IDENTITY THREAT DETECTION FOR OKTA

Real-time Threat Detection of Okta Identity Threats at Scale

Enterprise organizations have complex identity ecosystems stemming from the need to establish and maintain accurate user identities, access privileges, and permissions across multiple systems and platforms.

Managing this complexity and ensuring the integrity and security of the IAM system can be a significant challenge, with the sheer volume alone making it difficult to identify suspicious or abnormal behavior that could indicate a threat.

Organizations use identity and access management solutions like OKTA to address operational needs. However, from a security perspective, 75% of organizations who forward identity log sources to their SIEM do not use them for any detection use cases.* This leaves an organization vulnerable to identity-based threats. Why is this valuable data being collected but not used? The simple answer is legacy SIEM platforms are ill-equipped to provide actionable detections on this data. Rules and thresholds won't work.

MixMode Identity Threat Detection for Okta continuously monitors your Okta environment and correlates behavioral, access, and log data to detect attacks and lateral movement in real-time proactively.

How it Works

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 delivers tangible business outcomes in days and detects threats others miss in real-time.

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.

Enhanced Visibility

Contextual dashboards with AI-informed insights and detailed visibility.

Seamless Integration

No rules, training, onboarding, or tuning required; easily configurable API ingest.

Proven Scalability

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

MixMode's Identity Threat Detection seamlessly integrates with your Okta environment in minutes, providing a central location to view findings, analytics, and visualizations.

MixMode's patented Third Wave AI analyzes Okta log data in real-time to provide the following detections:

Active Users: Looks for risk in all user behaviors
Real-time and predictive dynamic threat detection for novel and known attacks at scale.

Login Geo Location: Looks for risk in users logging in from multiple locations (so-called impossible travel)
Detects potentially malicious activity by looking for successful logins from different geo-locations within a short amount of time.

Application Access: Looks for risk in user application access activity
Detects malicious insider or compromised credential activities around lateral movement across applications.

"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 Okta data in real-time.

Anomaly Detection
Helps identify threats that may not be apparent based solely on individual user behavior.

Detailed Investigations
Raw log querying for in-depth investigation and hunting exercises.

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

Advanced Analytics and Reporting
Actionable insights about network security posture, threat trends, and performance to make data-driven decisions.

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.