MixMode for Azure

The MixMode Platform detects anomalous activity within Microsoft Azure cloud environments by monitoring various Azure data sources, including Azure Activity Logs, Microsoft Entra ID (formerly Azure AD), and Azure Flow Logs, to identify threats through deviations from expected user and entity behavior.

Overview

In today's threat landscape, Microsoft, a cornerstone of business technology, is a prime target for sophisticated cyberattacks, continuously facing attacks by advanced threat actors (ATPs). This constant barrage translates to a heavy burden on security teams within organizations that rely on Microsoft Azure and Windows.

Managing thousands of security rules to keep pace is a never-ending battle. Furthermore, a significant portion of businesses using Microsoft Cloud and Office 365 products recognize the limitations of native security tools and the need to invest in additional advanced cybersecurity solutions.

Why Organizations Choose MixMode's Advanced Threat Detection for Azure

- **Legacy Security Can't Keep Up:** Traditional security solutions, including Microsoft Defender, struggle to identify advanced threats that leverage sophisticated techniques.
- **AI-Powered Adversaries:** Threat Actors are increasingly adopting AI to evade detection by traditional security tools. Their tactics can render signature-based approaches obsolete.
- **MixMode's AI Advantage:** MixMode's advanced Third-Wave AI goes beyond signatures. It proactively detects novel threats missed by most security solutions, providing superior protection for your Azure environment.

Key Features

- **AI-driven Anomaly Detection:** MixMode's AI utilizes dynamic models to establish continuous baselines for expected activity. Deviations from these baselines are flagged as potential security incidents
- **Entity and User Activity Monitoring:** Monitors API calls, application access, login attempts, and other activities performed by users and entities within Azure.
- **Azure Active Directory Integration:** Monitors user logins, application access attempts, and identifies potential compromised credentials or malicious insider activity.
- **Azure Flow Log Analysis:** Analyzes network traffic data for anomalies in total bytes transferred, rejected connections, and traffic direction (ingress, egress, inbound, outbound, local).
- **Alert Prioritization:** MixMode AI assigns risk scores to flagged events, helping security teams prioritize investigations based on potential severity.

Key Use Cases

Threat Detection and Prevention

- **Novel Attack Detection:** Identify unusual patterns in user and entity behavior, potentially indicating malicious activity to detect threats early, including ransomware.
- **Insider Threat Detection:** Monitor user actions to detect potential insider threats or data exfiltration.
- **Compromised Credential Detection:** Identify suspicious login activities and unauthorized application access.

Security Posture Improvement

- **Visibility and Monitoring:** Gain comprehensive visibility into user and entity activity within Azure.
- **Alert Prioritization:** Focus on high-priority threats by assigning deviation scores to alerts.
- **Compliance and Audit Support:** Meet compliance requirements by monitoring user and entity activity.

Operational Efficiency

- **Incident Response Acceleration:** Reduce investigation time by prioritizing alerts based on potential severity.