MixMode®

CASE STUDY

MixMode Uncovers Hidden Threats in Large Water and Power Company

The Challenge

A Large Water & Power Company (LEPC), a global leader in the Water sector, faced a daunting challenge in protecting its vast and complex IT infrastructure. Despite investing heavily in cybersecurity solutions, the company remained vulnerable to sophisticated threats. LEPC's existing security stack struggled to detect advanced persistent threats (APTs) and insider threats, leaving critical systems at risk.

The Solution

To bolster its cybersecurity defenses, LEPC initiated a proof-of-concept (POC) with MixMode, an advanced AI-driven threat detection platform. The goal of the POC was to compare and contrast the effectiveness, accuracy, and context provided by MixMode's autonomous platform against LEPC's existing cybersecurity solutions, processes, and personnel.

The Discovery

During the POC, The MixMode Platform was deployed in hours across LEPC's critical infrastructure. Within minutes, The Platform began building a comprehensive understanding of the network's normal behavior.

MixMode identified critical security vulnerabilities during the initial phase of deployment that included:

- **Weak network security management:** The network is exposed to significant risk due to the presence of cleartext passwords as well as privileged and restricted content, making it susceptible to man-in-the-middle attacks and unauthorized access.
- **Abnormal network traffic:** Previously undetected connections at significant volumes of inbound and outbound connections to known hostile geolocations indicate potential misconfigurations or active cyberattacks.
- **Active Directory vulnerabilities:** The network is vulnerable to Kerberoasting attacks, allowing threat actors to compromise service accounts.
- **Data exfiltration risks:** Attackers are using reverse tunneling techniques to establish covert communication channels, enabling data exfiltration and command-and-control activities.

Key Benefits

- **Rapid Threat Detection:** MixMode's advanced AI-powered capabilities enabled LEPC to identify hidden threats within minutes of deployment.
- **Enhanced Security Posture:** By augmenting LEPC's existing security stack, The MixMode Platform provided a comprehensive layer of protection against advanced threats.
- **Cost Savings:** Early detection and prevention of breaches helped LEPC avoid costly remediation efforts and reputational damage.
- **Improved Risk Management:** MixMode's continuous monitoring and advanced detection capabilities enabled LEPC to proactively manage risks and protect critical assets.

The Impact

The POC revealed critical gaps in LEPC's existing security infrastructure, as multiple threats were identified that had bypassed existing defenses. The MixMode Platform's ability to uncover these elusive threats underscores its effectiveness in detecting advanced attacks.

In addition, LEPC's SOC team experienced a greater than 90% reduction of alerts from Day 1 to Day 5 in favor of autonomously prioritized, context-rich detections and continued to show improvement throughout the POC.

Advanced AI-Powered Detection for All

Impressed by the results, LEPC decided to fully deploy MixMode across its entire enterprise. By implementing MixMode, LEPC gained a significant advantage in its battle against cyber threats. The MixMode Platform's continuous monitoring and real-time detection capabilities enabled the company to proactively identify and mitigate risks, reducing the likelihood of successful attacks and minimizing potential financial losses.

Conclusion

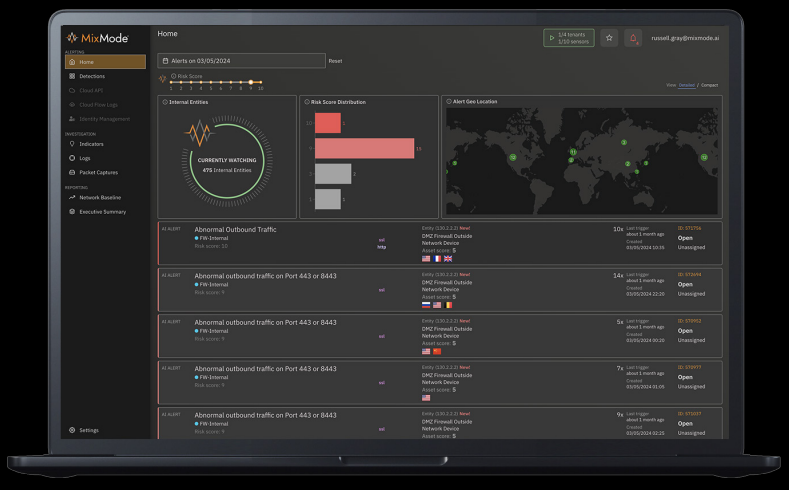
LEPC's partnership with MixMode exemplifies the power of advanced AI-driven cybersecurity. By leveraging MixMode's innovative Platform, the company successfully addressed a critical security gap and strengthened its overall security posture. The case highlights the importance of adopting advanced technologies to combat the evolving threat landscape.

In less than 72 hours, The MixMode Platform identified an attack in progress that had evaded LEPC's existing security tools.

This stealthy adversary had infiltrated the network and had begun to try exfiltrating sensitive data.

The MixMode Platform's advanced detection capabilities uncovered the threat before it could escalate into a full-blown breach.

Advanced Threat Detection Prioritized for YOUR Environment



About MixMode: MixMode is the leader in AI-driven dynamical threat detection solutions, delivering a patented, self-learning platform designed to detect both known and unknown threats across cloud, hybrid, or on-prem environments. Large enterprises with big data environments, including global entities in financial services, public utilities, 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.