MixMode®

CASE STUDY

Securing the Grid: How a Major Utility Leveraged MixMode's AI to Safeguard Critical Infrastructure

Confronting the Limitations of Traditional Cybersecurity

For a large US utility company, the stakes couldn't be higher. As the guardian of a vital regional energy grid, any breach or disruption to their network could have catastrophic real-world consequences. Yet, despite their substantial investments in security solutions, the utility's cybersecurity team found themselves increasingly hamstrung by the limitations of their existing tools.

The Challenge

The enterprise's SIEM platform, shared across multiple teams, needed to be improved to meet the specialized needs of the security operations center (SOC). While the compliance team deemed the system satisfactory, the cybersecurity group was stifled by its inability to perform fundamental tasks:

- Identify and detect real-time network traffic anomalies that could indicate state-sponsored attacks
- Alert on critical policy violations and misconfigurations threatening the network
- Detect adversarial AI attacks and collaborative hacker activity
- Develop a robust, continuously evolving baseline of expected network behaviors

Worse, the utility's sprawling, hybrid infrastructure—encompassing legacy systems, cloud environments, and on-premises resources—further exacerbated the challenges, pushing the SIEM platform beyond its capabilities.

As one manager explained, "Vendor promises evaporate when the realities of their complex networks push the bounds of what a traditional SIEM and NTA can deliver." The utility needed a fresh approach to bridge the inherent gaps in its security architecture without disrupting its critical operations.

The Results

- **Visibility into Advanced Threats**: The MixMode Platform immediately identified adversarial AI attacks, state-sponsored intrusions, and other sophisticated threats evading the utility's existing security solutions.
- **Reduced False Positives:** The MixMode Platform slashed false positive rates by over 95% by understanding network usage and establishing an evolving baseline of regular network activity.
- **Streamlined Operations:** The utility shifted core SOC and network monitoring responsibilities to The MixMode Platform, freeing up valuable resources.AI-driven approach.

The Results: Regaining Control, Slashing Costs

Determined to fortify their network defenses, the utility turned to MixMode, the leader in delivering advanced AI cybersecurity solutions for real-time threat detection and response at scale. Unlike conventional security tools reliant on rigid rules and thresholds, MixMode's advanced AI continuously analyzes real-time network behavior, dynamically adapting to detect anomalies and predict future threats.

Within a single day of deployment, The MixMode Platform began delivering transformative results:

- **Visibility into Advanced Threats:** The MixMode Platform immediately identified adversarial AI attacks, state-sponsored intrusions, and other sophisticated threats evading the utility's existing security solutions.
- **Reduced False Positives:** The MixMode Platform slashed false positive rates by over 95% by understanding network usage and establishing an evolving baseline of regular network activity.
- **Streamlined Operations:** The utility shifted core SOC and network monitoring responsibilities to The MixMode Platform, freeing up valuable resources.

"MixMode was able to draw attention to what we had suspected all along with views into adversarial AI and state-sponsored attacks, including attacks originated from suspicious geographies—and they delivered this insight on Day One," remarked a member of the security team.

Unlocking Utility-Wide Benefits

The utility's leadership was so impressed with The MixMode Platform's capabilities that they expanded the deployment, shifting core functional requirements from their SIEM to the AI-powered platform. Not only did this deliver superior security outcomes, but it also unlocked substantial cost savings.

"We were not only able to save money, we were able to actually retrieve budget by deploying MixMode and reallocate that budget more effectively while better addressing the functional requirements of the deployment across our different lines of business," explained a manager.

The utility dramatically decreased its overall data storage and processing costs by reducing the traffic flowing to its SIEM system. As importantly, MixMode's AI-first approach provided heightened visibility and granularity, empowering the security and networking teams to proactively safeguard the critical infrastructure.

As threats to the energy grid continue to escalate, utilities can no longer rely on outdated, rules-based security tools. With MixMode's AI-powered platform, this forward-thinking utility has transformed its cybersecurity capabilities, positioning itself to meet the evolving challenges of today and tomorrow.

"MixMode has given us more insights and value than any tool we have ever deployed"

Major Utility
Manager

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.