

# WHY A LARGE US UTILITY COMPANY TURNED TO MIXMODE TO ADDRESS UTILITY GRID VULNERABILITIES

## MixMode Results:

- Decreased total SIEM deployment cost by decreasing the amount of traffic that needed to be aggregated and stored
- Shift from a dependency on rules- and threshold-based approaches for security operations teams on the front line to turning all of that functional responsibility to MixMode
- Identify state-sponsored attacks from foreign entities that they had no visibility into with their SIEM-based rules and threshold-based approach
- Identify policy violations and active adversarial AI attacks
- AI-first, full-fidelity forensic search and investigative functionality
- MixMode deployed, operational and providing generative baseline AI-informed insights and alerts in one day
- Fully self-supervised and self-tuned with demonstrable AI learning in one week
- >95% Reduction in false positives

## The Challenge

A large utility company approached MixMode with the following scenario: The enterprise SOC was utilizing a shared SIEM application that was being utilized by several stakeholders: the networking team, the SCADA team, the dev-ops team, the compliance team and cybersecurity teams for “basic search and investigation of log files to meet regulatory compliance requirements”. Although the compliance team at this utility found the SIEM satisfactory, the cybersecurity team was hindered by the system’s inability to perform several fundamental functions including its ability to:

- Identify and detect real-time network traffic analysis and variations they suspected would be reflective of state-sponsored attacks
- Alert on policy violations and network misconfigurations that represent serious threats to the organization
- Detect adversarial AI attacks
- Detect individual or collaborative hacker attacks taking place on a daily basis
- Develop a baseline of expected network behaviors based on a continually evolving baseline
- Adequately monitor a mix of legacy systems, cloud data and on-prem resources

The seriousness of these fundamental failings was further underscored by the fact that the regional utility grid infrastructure was at risk. A serious breach could mean a major real world threat to an entire region, should the utility grid become compromised through an attack.

The utility company explored various SIEM and NTA based options to address their network security needs, but it became clear to them that leaders in the space were unable to address these issues. Vendor promises evaporate when the realities of their complex networks push the bounds of what a traditional SIEM and NTA deliver.

Large organizations face unique challenges, especially as it relates to infrastructure. Entities similar to this large utility company must reconcile dueling goals competing within a shared framework. At first a one-size-fits-all approach may seem straightforward and effective.

Often, network security at these sprawling organizations is vulnerable partly because the approach has been a patchwork of ad hoc fixes. It can become so challenging to unravel the complex nature of these security puzzles that a fresh start may seem like the only viable path forward. The reality, however, is that very few large enterprise operations have the ability to dedicate the financial, time, or labor resources to start from scratch. Entities like our utility customer can’t simply toss aside the legacy systems they rely on to perform fundamental tasks.

## MixMode Was Able to Identify:

- Adversarial AI and active attacks the utility had suspected, which had gone undetected by their SIEM deployment
- Network misconfigurations
- Active attacks, threats, and vulnerabilities
- Adherence-to-policy issues on the networking side

***"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 delivered this insight on Day One."***

## Barriers to Successful Network Oversight

The only truly workable network solution must bridge the inherent gaps that exist throughout these systems. It must also be capable enough to root out hidden vulnerabilities ripe for hacking.

Customers that approach MixMode at this stage have undoubtedly tried other network security solutions over the years, in particular standalone SIEM products, with varying levels of success.

Perhaps most frustrating to this large utility company is that their network security wishlist is not focused on lofty, unattainable goals. The problem is not that the customer is asking for too much. The problem is that their SIEM products are not capable of achieving simple fundamental tasks on their own, even with expensive add-ons.

Organizations operating these complex, decentralized systems stand to reap big benefits from a solution that adds centralization without disturbing their distributed needs. Rather than going through the large task of adapting their systems to a network security solution, they need a solution that meets them where they are.

## The Solution

The utility company was not satisfied with the typical vendor approach that urged them to simply trust the output of the capabilities of their platforms. The platforms had been pre-configured and pre-tuned by the vendors themselves. They were unsatisfied with the pre-delivered dashboards and pre-delivered analytics that would require additional work toward validation.

In a way, the outcome would be a "watcher of watchers" approach, and still not deliver the necessary level of oversight. They would need to embark on a multi-step validation process in order to achieve information they could glean from MixMode with a limited time investment:

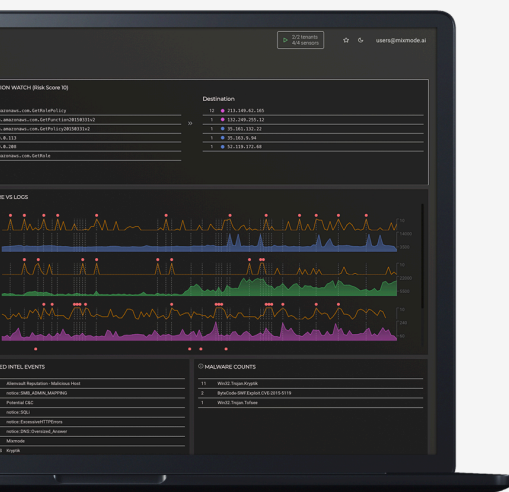
- Validate the output of the AI
- Demonstrate how the AI operates
- Demonstrate the AI's ability to be turned on or off by the operator for comparative purposes
- Provide full forensic search and investigative capabilities of network traffic and log details

Historically, these log details had been relegated to SIEM deployment.

The utility performed a head-to-head comparison of the rules-based approach and dashboard functionality offered by SIEM vendors to those offered by MixMode, ultimately determining that MixMode was far more effective. They then chose to turn to MixMode to prepare a proof of concept that served as a phase-one deployment directly into their production environment.

Given the sensitivity of the company's network data, MixMode was granted only limited access. Within a single day, the team had installed and configured the MixMode platform in production, without human operator involvement from the utility's teams.

***“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.”***



## The Results

The utility's leadership team was so impressed with the MixMode solution that they were able to lift all the functional requirements for their security and networking teams related to SIEM deployment and shift those functional requirements to MixMode.

Ultimately, the utility determined that MixMode provided a far greater level of visibility and granularity to both the network and security teams while decreasing the traffic flow to their SIEM system.

When the leadership team studied the output, as validated by the security team, the picture became clear. MixMode was an essential application that needed to stay in production and further deployed immediately. The MixMode team was able to expand the scope of the proof of concept to roll out the system to a larger capacity, versus going offline for a period. This allowed the utility to retain visibility into NTA throughout procurement.

***“By shifting to a purpose-built platform to address our functional requirements we were able to decrease the costs and ingests by so much that we were able to recoup costs.”***

## Compliance Improvements

Another significant challenge facing our large utility company customer is adhering to strict industry compliance requirements. SIEM vendors sometimes fail to mention that while compliance benefits are possible with their product, they will significantly increase costs. MixMode delivers compliance benefits by decreasing the amount of traffic that flows to the SIEM for legacy compliance purposes while providing additive functional capabilities for networking and security teams on the front end. Ultimately, this is a zero-cost model.

***“MixMode has given us more insights and value than any tool we have ever deployed.”***

## How Can MixMode Help You?

Customers routinely encounter aggressive SIEM vendors who encourage them to consider adding IT operational intelligence as an additional SIEM platform deliverable. They do this by creating layer upon layer of abstraction, normalization, reporting, queries, thresholds-based alerts and dashboards, which all come at a premium.

Ultimately, the MixMode platform addresses a host of challenges with our single purpose-built solution that serves both security operation teams and network operation centers. The challenges of traditional SOC, UBA and SIEM as well as those associated with traditional network operation centers are all overcome with the singular MixMode platform.

To learn more about MixMode's next-generation AI-powered cybersecurity platform contact us to schedule a consultation and demo.