WHY A LARGE GOVERNMENT ENTITY REPLACED THEIR SIEM WITH MIXMODE

Deployment Objectives:

- Demonstrate MixMode's AI abilities to establish a generative, evolving baseline of appropriate network traffic behavior.
- Demonstrate MixMode's ability to identify true positives and anomalies leveraging 3rd Wave Artificial Intelligence.
- Demonstrate MixMode's ability to suppress false positives while identifying and elevating true positives and threat intelligence.
- Reduce or eliminate dependency on human operators for deployment, maintenance, configuration and tuning of the system with MixMode's 3rd Wave Artificial Intelligence.

The Challenge

Many customers come to MixMode with a very specific business problem when it comes to their SIEM and accompanying cybersecurity platforms. It can be summed up in a quote from a senior security professional working in the SOC of a large government entity: "I'm trying to address the same functional requirements today that I was trying to address 15 years ago, and these systems have proven ineffective at addressing not only my functional requirements but they've also created operational and technology costs that are unsustainable."

One client, a large government entity, came to MixMode with a similar issue. Despite a three-year SIEM deployment and a two-year UBA deployment, government personnel needed an alternative to better detect and manage threats in real-time, as well as an improved platform for gathering comprehensive data. A large problem with the SIEM and UBA technology used by the government entity was they monitor different data and did not communicate with each other, resulting in the constant need to reconfigure each tool and aggregate data. Managing both the SIEM and UBA platforms was becoming too costly to continue.

> *"The resource requirements to continually define, modify and optimize those sources of data for the particular use cases became an operational challenge in that we just didn't have teams of advanced security experts to continually optimize these systems."*

Insider threat prevention was another major challenge. Despite the presence of their UBA platform, they suspected there were internal actors, technologies and policy violations that represented a significant risk. The UBA platform had proven ineffective at identifying these threats and anomalies.

Deployment Results:

- MixMode deployed, operational and providing generative baseline AI-informed insights and alerts in 1 day.
- Fully self-supervised and self-tuned with demonstrable AI learning in 1-week.
- Additive east/west network traffic visibility and AI-informed alerting deployed and operational in production in ~1 hour.
- >95% reduction in false positives in week 1.
- AI-informed validation of procedures and controls.
- AI-informed visibility into network optimization and configuration.
- AI-informed visibility and anomaly detection on syslog (SIEM replacement).
- True positive threat identification without human operator, tuning or intervention.
- AI-first, full-fidelity forensic search and investigative functionality in production.

The Solution

MixMode worked with the government entity to deploy a next-generation SOC platform using 3rd Wave Artificial Intelligence to address both their SIEM and UBA requirements. Within the first 24-hours, MixMode was able to demonstrate better granularity and authentic visibility into real-time threats as they occurred as well as network and operational configuration challenges.

A manager associated with the project stated, “Traditional log aggregation approaches from rule-based systems don't have any real insights. The predefined queries and dashboards lack the alerts that one would need to identify insider threats. They're all just for east-west types of threats and anomalies in network infrastructure.”

Government personnel were not needed to configure the SOC, since MixMode’s technology configures itself, which offered a solution to one of the most cost-prohibitive components of the systems that they previously had in place.

“Within the first 24-hour learning period, literally one day after the installation, the AI platform was delivering better accuracy, granularity, visibility, and consumable information for business and non-technical audiences than our SIEM and UBA.”

The Results

The new platform and its level of visibility allowed the government entity to become more agile and responsive, so much so that they decided to decommission both the legacy UBA and SIEM systems in favor of a next-generation SOC powered by MixMode.

As a government entity, they had a unique need to comply with requirements like PCI and HIPAA. With MixMode, they were able to meet these requirements with ease, using a single platform. MixMode allowed them to demonstrate they had the capability to go back and access required data and provide forensic-level detail about it. They were able to get that visibility in one week without any resource involvement whatsoever, purely based on the artificial intelligence-informed insights that they were able to achieve.

“One of the most common failings I have seen is a SIEM overstuffed with useless data. A SIEM should augment analysis, not hinder it. Put simply: less is more. The more data you have, the worse the SIEM performs.”

- Justin Henderson, SANS Institute

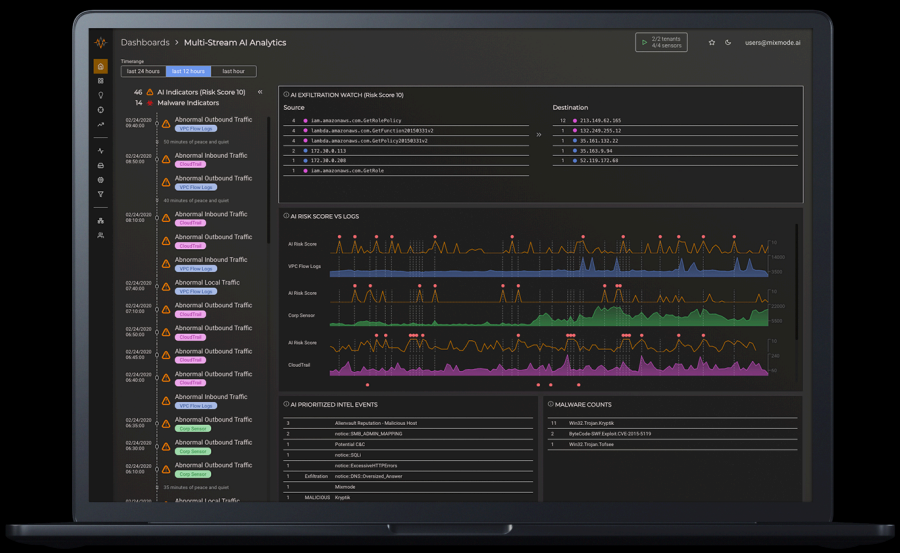
"We were not only able to save money, we were able to actually retrieve budget by deploying MixMode and reallocate that budget more effectively while better addressing the functional requirements of the deployment across our different lines of business."

Previously, they had put into place a large collection of rules-based alerts, queries and dashboards that had been designed to provide threat intelligence via the SIEM. Because that information was based on legacy log data, they had no visibility into real-time threats and anomalies. MixMode was able to identify active attacks and probes that were taking place that the customer's existing tools had no visibility into, confirming the customer's suspicions. In particular, insider behaviors came into clear view.

Within a week, MixMode was able to address the immediate functional requirements related to security challenges as well as addressing the previously unknown network configuration and optimization challenges, without any operational resources, predefined queries, pre-existing intel feeds or rules-based alerts.

Government personnel saw immediate benefit in using the platform, being able to identify real time threats and anomalies, as well as quickly analyze data. They found the platform's functionality and quality of data to be useful to them both immediately and in the future. Additionally, the self-sustaining nature of the SOC platform eliminated extreme costs associated with the added human resources that had previously been necessary to configure and manage the SIEM and UBA systems.

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



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.