MixMode

# HOW THE FIFTH LARGEST U.S. CITY RAPIDLY MODERNIZED ITS CYBERSECURITY DEFENSES

**Learn how the City of Phoenix cut its cyber tool footprint in half, gained visibility into advanced foreign adversary attacks, and greatly improved the productivity of its SOC staff.**

City of Phoenix

## The Challenge

The City of Phoenix's cybersecurity leaders, Shannon Lawson and Mitch Kohlbecher, have been at the forefront of adopting new technology to solve the fundamental problem perplexing cybersecurity leaders everywhere: how can we reduce our ever-expanding, costly and inefficient cyber tool footprint while also increasing the effectiveness of our cyber defenses and the productivity of our lean SOC team?

With years of experience as a veteran cybersecurity leader, Shannon described this fundamental problem faced by all CISOs explaining, **"For 15 years I have been trying to implement a cyber defense that surfaces increasingly sophisticated threats in real-time, with the least amount of maintenance and cost. This problem has grown exponentially with exploding cloud utilization, architecture and network complexities. The good guys have fallen too far behind the advanced threat actors."**

When the City of Phoenix's leadership team was approached by a Federal agency notifying them of active targeting by a foreign nation state sponsored threat actor using advanced techniques designed to circumvent traditional rule and threshold-based cybersecurity tools, Shannon knew the City could no longer rely on its expansive, costly and ineffective legacy systems. The City's existing cybersecurity platforms failed to detect advanced attacks, despite ever increasing IT investments in these legacy tools and the required training and certifications of their SOC team to use them.

## Challenges

1. City had no means of detecting novel or sophisticated threats
2. Too many tools and no ability to correlate across a large complex environment
3. City was facing a massive shortage of cyber professionals

## Results

1. Immediately able to detect novel threats from foreign countries
2. Intelligent correlation of alerts and events across many disparate data sources
3. SOC team performs more effectively with less resources
4. Realized long-term modernization goals for cyber defense with no additional cost

The primary reasons the City was failing to detect these novel threats are common across the industry:

1. **The City had no means of detecting "novel", or never before seen attacks.** The tools in place at the City had no ability to detect cyberthreats that were not in a threat intel feed or detectable by a rule they had written. This was leaving the City vulnerable to 80% of potential attacks.
2. **Multiple cybersecurity tools monitoring different data sets.** These tools did not communicate with each other, requiring constant reconfiguration and manual triaging of aggregate data.
3. **The SIEM licensing model made it overly expensive and impractical to collect relevant events and logs.** Gartner outlined this problem in a recent report noting that organizations that lack sufficient budgets to expand their existing SIEM solutions must choose between deprioritizing existing use cases, not adding new use cases or decreasing the scope of monitoring.
4. **Finding, hiring and retaining cybersecurity professionals.** The City was constantly swimming against the current to hire employees with dedicated experience using SIEM or UEBA tools. These are costly employee roles, compounded by the constant headhunting by larger corporations, resulting in salary demands that cities struggle to fit into their pay scales. To add to the staffing challenges, even the most experienced and well-trained cybersecurity professionals struggle to be effective when they spend the majority of their day chasing down and interpreting false-positive alerts from multiple, nonintegrated tools.

## The Solution

MixMode worked with the City of Phoenix's cybersecurity team to deploy a next-generation SOC platform using Self-Learning Artificial Intelligence to enable real-time visibility into all threats and anomalies in their network, both known and novel (like zero-days), consolidate their legacy toolset, and improve the productivity of their SOC team.

Within the first 24 hours of deployment, absent any human operator involvement, MixMode provided visibility into and context for active, real-time attacks as well as network and configuration inadequacies that had gone undetected by all their other cybersecurity tools and their human operators. The visibility that MixMode provided in those first 24hrs resulted in the City taking immediate action to resolve the issues and ultimately strengthen its defenses. By eliminating unnecessary SIEM and UEBA costs, Phoenix was able to fully fund the MixMode deployment, gaining real-time and novel threat detection, without losing the functionality they got from their SIEM and UEBA deployments.

Since MixMode's self-learning AI technology configures itself, the SOC team was able to quickly deploy the solution and avoid the lengthy amount of time and high cost typical of most other cybersecurity tools deployments. In fact, MixMode was deployed in under an hour without any professional services, training, tuning, or data management. Within the first 48 hours of deployment the CISO invited MixMode to expand the deployment to identify internal threats and anomalies their legacy cybersecurity tools had failed to detect. In addition to north-south threats, an expansion to monitoring east-west and internal threats helped to identify insider threats before any damage could be done as well.

*"MixMode was deployed remotely in under an hour and detected threats on day 1 that other platforms and their human operators had missed. MixMode's AI platform is now the core intelligence layer for our Security Operations Center"*

**Shannon Lawson**
CISO, City of Phoenix

## The Result

Within 72 hours after the initial deployment, the team was able to shut down active threats that posed a risk to the organization by identifying anomalous behaviors and supporting context that their legacy tools weren't detecting. During the expanded deployment, the City used MixMode to identify any nefarious, suspicious, or anomalous activity deriving from nation-states including Russia and China.

MixMode's platform was able to immediately identify potential insider threat activity, never seen before outside threats and exfiltration activity that had gone completely undetected by the previous SIEM and UEBA systems. The City of Phoenix now had the precise information needed to secure their environment.

*"The MixMode platform was live and delivering insights other platforms had missed within 24 hours"*

**Mitch Kohlbecher**
Deputy CISO, City of Phoenix

The addition of a modern cybersecurity platform and its level of visibility allowed Phoenix to become more agile and responsive, so much so that they decided to decommission both the legacy UEBA and SIEM systems in favor of a next-generation SOC powered by MixMode. When asked about MixMode, Mitch Kohlbecher, Deputy CISO said, "We were initially quite skeptical of MixMode's claim to be fully deployed and operational absent any human operator involvement within 1 week. The MixMode platform was live and delivering insights other platforms had missed within 24 hours." As a government entity, they had additional PCI and HIPAA compliance requirements. With MixMode, the City was able to meet these requirements, increase visibility significantly, and enable more effective threat detection with ease, using a single platform.

MixMode's ability to identify suspicious behaviors with accuracy, precision, and context gave the organization visibility into what was happening in the City's environment at a granular level and the insights necessary to address and resolve issues well beyond the capabilities of the City's prior tools, including its limited human resources, ultimately meeting and exceeding the CISO's desired SOC needs.

### MixMode's 24/7 Managed SOC Approach

The City of Phoenix's deployment of MixMode included 24/7 managed SOC services to augment and bolster the City's strained SOC team. This supplementary SOC service included hourly and daily AI informed alerts, threats, risks, and anomalies, as well as guided recommendations and best practices for remediation and attack prevention. Effectively, the City quadrupled the size of their SOC team and exponentially increased the strained internal SOC team's effectiveness without any increase in cost or resources.

MixMode also provided the City with executive reports detailing the potential impact of impending threats, including those involved in the coordinated nation-state attacks. This helped to raise awareness across other City departments, utility providers, and other entities at risk of becoming unable to provide sufficient community support for core functions, should they be targeted by an attack. Soon, several other departments took notice and looked to adopt the MixMode platform.

As a result, the City of Phoenix's leadership decided to offer these departments a central SOC powered by MixMode. Today these City critical infrastructure departments are participating in a shared services model which provides managed Cybersecurity built entirely upon MixMode. This shared services model has materially reduced the resource requirements for each individual department to manage operational resources and technology maintenance while broadly increasing the efficacy of their cyber defenses.

## About MixMode

The MixMode platform is the first cybersecurity platform to leverage "Third Wave" AI (as defined by DARPA), utilizing an advanced self-supervised learning model to surface both known and novel attacks, as well as misconfigurations and other vulnerabilities. This self-supervised approach is led by MixMode's CTO and chief scientist, Dr. Igor Mezic, who has 20+ years of experience developing advanced AI technology that has been used for projects with DARPA, Air Force, Army, CDC and many others. MixMode is used across many industries and addresses the needs of customers for various use cases, including: NTA, UEBA, NDR and/or SIEM. The company is headquartered in Santa Barbara, CA. Visit us at www.mixmode.ai.

## Results

1. **The City was able to immediately detect novel threats from foreign countries that legacy platforms missed.**
2. **The City was able to replace multiple expensive legacy cybersecurity platforms straining limited SOC resources.**
3. **The City has one platform that provides intelligent correlation of alerts and events across many disparate data sources.**
4. **The City's SOC team is performing more effectively than ever with less resources.**
5. **The City realized its long-term modernization goals for its cybersecurity defense, fully funding the transformational deployment through its consolidation of tools and reduction of storage and licensing costs.**