MixMode®

CASE STUDY

Revolutionizing Threat Detection for a Major Metropolitan Area

The Challenge

One of the largest metropolitan areas in the United States found itself under siege from a sophisticated cyberattack launched by foreign adversaries. This incident underscored a critical gap in the city's threat detection capabilities. Simultaneously, the rapid growth and complexity of the city's data environment placed an immense strain on the security team, hindering their ability to effectively identify and respond to potential threats.

The Solution

Central to its mitigation efforts, the city implemented The MixMode Platform, a cutting-edge threat detection solution powered by the most advanced artificial intelligence in the world, Third Wave AI. The MixMode Platform across its critical network infrastructure, including the DMZ, the city significantly enhanced its overall security posture and dramatically improved its threat detection capabilities immediately.

The deployment of The MixMode Platform yielded impressive results:

- **Dramatic reduction in investigation time:** The MixMode Platform saved the security team an estimated $5 million in investigation hours.
- **Enhanced threat detection:** By leveraging its unique negative time-to-detection capabilities, The MixMode Platform enabled the team to identify potential threats before they escalated into incidents, significantly reducing risk.
- **Significant reduction in false positives:** The MixMode Platform effectively filtered out noise, saving the security team over 50,000 hours of investigating irrelevant alerts and allowing them to focus on high-priority threats.
- **Improved threat hunting:** The MixMode Platform empowered the security team to investigate and contain over 31,000 elevated threats, demonstrating its effectiveness in identifying and responding to advanced cyber threat activity .
- **Strengthened defenses against targeted attacks:** The MixMode Platform identified and contained over 102,000 connections originating from high-risk regions (including China and Russia), protecting critical infrastructure from potential compromise.

The Results

- **$5 million** saved in investigation hours
- **31,000+** elevated cyber threats searched and investigated
- **50,000+** cyber threat search and investigation hours saved
- **102,000+** connections with China and Russia identified and contained

The Impact

By adopting The MixMode Platform, the city has achieved a significant leap forward in its cybersecurity capabilities. The Platform's ability to detect advanced threats early, significantly reduce false positives, and automate routine tasks has empowered the city's security team to focus on strategic initiatives and proactively defend against emerging threats. The city is now better equipped to protect its critical infrastructure and citizen data from sophisticated cyberattacks.