MixMode

SELF-LEARNING CYBER DEFENSE FOR FINANCIAL SERVICES INSTITUTIONS

Learn how a large Financial Services Institution deployed MixMode to ingest and analyze otherwise unmanageable volumes of cloud-based data, identified active, novel attacks designed to bypass existing cybersecurity platforms, and unburdened its security team from writing rules within the first week of deployment.

The country's largest Financial Services companies are a favorite target for nation-state sponsored and coordinated cyberattacks to cause economic damage and disruption. Despite a significantly larger investment in Cybersecurity than almost any other industry, breaches and successful novel attacks against these organizations still remain a daily occurrence.

Contributing to this issue are the legacy Cybersecurity tools in place at these organizations and their technical limitations in attack detection and scalability. These tools were designed to focus on the long-term storage of data, with perpetual data management and proprietary storage formats, but were not designed to quickly detect attacks across multiple platforms and teams. Financial Services providers need real-time detection of threats, and existing rules-dependent tools fall short.

MixMode Predicts & Detects Attacks that Legacy Platforms Miss

MixMode was approached by a large Financial Services Institution facing these challenges, following a long search for a solution to detect novel attacks without relying on rules. Many large Financial Services enterprises spend in excess of $100M on Cybersecurity tools and supporting teams per year, yet breaches continue to succeed, most utilizing sophisticated, novel attack techniques designed to go around rules-based systems.

Challenges

1. Novel attack techniques that had gone undetected by rule-based systems.
2. Excess of 55,000 network traffic alerts every 15 minutes, all day, every day.
3. Data volumes that could not be managed by traditional cybersecurity tools.

Results

1. Identification of active, novel attacks the bank's other platforms had missed.
2. Reduction in false positives exceeding 95% within the first week of the deployment.
3. Deployed remotely, with no required hardware, in under an hour without any historical data, training, tuning, labeling, rules or any human operator involvement.

In this particular case, the alert volume generated by the bank's existing cyber tools was compounding the problem, resulting in more than 50,000 network traffic alerts every 15 minutes, all day, every day. These rule-based alerts, overwhelmingly false positives, were impossible for the Cybersecurity team to manage – and as a result, the search for novel attacks becomes a manual process at most large enterprises. Unfortunately, this was the existing state of affairs even before the bank's requirement to include monitoring of public cloud data. These additional data sources amounted to more than 500,000 events per second, a volume that could not be managed by any of the existing Cybersecurity tools in place. Simply put, the bank's existing Cybersecurity program did not have platforms in place to effectively manage the data in the system.

The use case the bank put forth to MixMode was simple, yet difficult to find in this industry. The bank needed a platform that could: (1) effectively and efficiently ingest the data volumes in its system; and (2) surface critical alerts including on novel attacks, without delivering a sea of false positives.

The above goals had proven to be unattainable using traditional SIEM, UEBA, NDR, and NTA platforms, including those powered by machine learning (which are generally rules-based systems that cannot effectively provide alerting on zero-day attacks). The objective was to enable identification, notification, and context for the bank's highest-risk threats and to detect anomalies in real-time, absent any human operator involvement, data training, or tuning. Similarly, because these sophisticated attacks do not have signatures and are unknown before they occur, a SOC team cannot write rules against these attacks. As this bank told us: "We cannot hire an infinite number of SOC analysts to write a never-ending list of rules to address every permutation of a new potential attack. We need a system that does not need rules to see novel attacks." Therefore, the bank was looking for a platform **with no dependency on rules to surface known or novel attacks.**

Beyond the surfacing of these alerts, the bank required real-time visibility and supporting context for critical Cybersecurity events, inclusive of massive amounts of both on-premise and public cloud data. Challenged by the limitations of traditional cloud monitoring systems which primarily measured only connection volume information, the bank required detailed information about inbound and outbound connections, access granted vs access denied analytics, corresponding ingress, egress, and lateral movement events, associated accepted and/or rejected connections, and identification of anomalous time-periods. All of these variables must also include contributing contextual data including data volume, content, and specific entities involved, delineated by time period, all regardless of the data type or format. For the last couple of years, the bank had been looking for a solution along these lines that included research and testing of "every traditional Cybersecurity tool on the market".

The Deployment and Results - Immediate Improvement in Efficiency & Effectiveness

The bank's goals were achieved with no use of rules. The MixMode platform was deployed remotely, with no proprietary appliances, in under an hour. With MixMode, the bank was able to achieve the following business outcomes:

1. Ability to ingest and analyze hundreds of billions of records of Cloud Flow Logs and API data.
2. MixMode identified anomalous behaviors, and then automatically appended relevant contextual insights, enabling the identification and investigation of Cloud Flow threats that had not been possible before.
3. Achieved an immediate efficiency gain: reducing false positives by over 96% within the first week of the deployment.
4. Able to parse through the flood of access denied errors to identify potentially anomalous or malicious behaviors.
5. Notably, MixMode surfaced active, novel attacks the bank's other rule-based platforms had missed.

Because MixMode is a self-learning, generative platform, all of this was accomplished absent any rules, historical data, training, tuning, labeling, or any human operator involvement. The bank was also not required to hire a team of "MixMode Specialists" to come in and deploy, configure and maintain the system (typical with many Cybersecurity vendors). Building on this initial success, MixMode has partnered with the bank to add context and understanding essential to comprehensive threat detection for a complex organization of this size.

Summary - Intelligence Achieved

As advanced cyber threats continue to evolve, and sophisticated, nation-state sponsored attacks increase, **Financial Services companies must be able to detect these novel attacks in real-time, regardless of data type, format or volumes.** With an acknowledgement that SOC teams cannot write an infinite number of rules to address novel attacks, leading Financial Services institutions are seeking out more effective solutions that can automate the process of finding novel attacks, zero day attacks and low and slow attacks. The bank's deployment of MixMode's self-supervised, no rules platform has saved their analysts from endless hours of writing rules and proven demonstrably more effective at addressing modern Cybersecurity threats than any previously available technology. To learn more, please visit us at www.mixmode.ai.