MixMode™

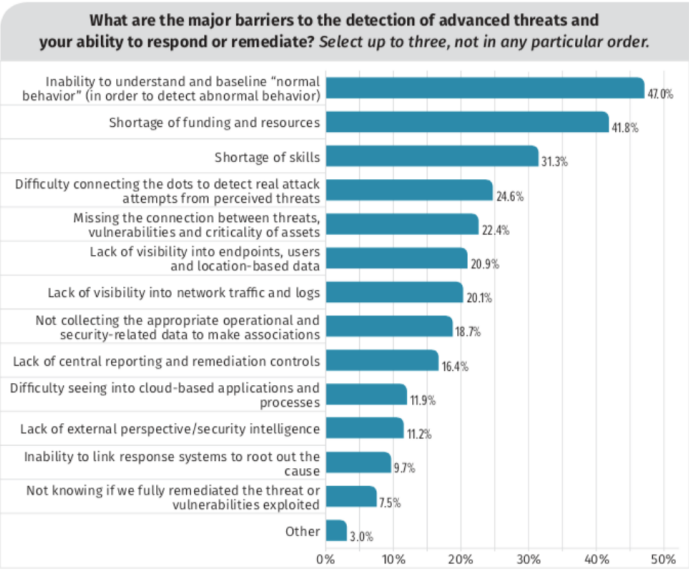
ACTIONABLE ANOMALIES

How MixMode AI Makes Your Security Data Smarter

By Russell Gray

In today's ever evolving cybersecurity landscape there are major problems facing professionals that continue to worsen. These problems center around a shortage of tools advanced enough to understand the baseline of a network in order to pinpoint anomalies and a massive information overload problem in the form of security alerts.

In a recent report by the SANS institute, a study showed that for most security teams the number one barrier to the detection of advanced threats and the ability to respond was a lack of understanding of "normal behavior" or a baseline of what is normal behavior on the network.



This is due not only to a lack of tools with the advanced capability to provide this baseline, but also, according to the same SANS study, "a lack of data integration between current security analytics tools and cloud infrastructure."

Unfortunately, traditional security tools are time-consuming, if not impossible, to tune for alert accuracy. This creates an ever-increasing problem of having too many alerts for your under-resourced security teams to investigate. In fact, for companies over 500 employees, enterprise security teams have six, or more, different security systems generating over 3,400 security alerts a day.

Given the volume of security noise, and the lack of human resources, it is not surprising that 32% of security professionals admit to ignoring alerts. A dangerous trend that is born out of sheer necessity. The trending in cybersecurity further supports this assessment. When reviewing the rate at which the annual spend in cybersecurity increases each year, one would expect the rate and severity of breaches to be shrinking or at least holding steady, however, this is not the case.

In 2019 the number of cybersecurity breaches increased by 17% (MarketWatch). Put more plainly the cybersecurity industry now seems to be meeting Einstein's definition of insanity, "doing the same thing over and over again and expecting different results." The volume of alerts proliferated by unactionable data is at the root of this problem.

How MixMode is Working to Fix It

MixMode created its proprietary, third-wave Artificial Intelligence to solve the problem of security alert fatigue by reducing the number of false positive alerts produced. Rule and threshold-based alerting tools are proven to be 20x less effective than AI based tools that correlate intel-based alerts with anomaly detection.

This increased volume is both time-consuming and dangerous. According to the Ponemon Institute, the average company of over 500 employees wastes the equivalent of 10 full time employees chasing erroneous alerts. What's more, a full 30% of cybersecurity professionals admit to ignoring alerts due to volume.

MixMode's approach to cybersecurity addresses both of these concerns by filtering out false-positive alerts, reducing the occurrence of false-negatives and allowing your security to focus on alerts that are actionable.

MixMode's AI is proprietary and is different than any other AI in cybersecurity. Our third-wave unsupervised learning engine was purpose-built for cybersecurity. Our AI evaluates your network's dynamic behavioral patterns and establishes a baseline for normal business operations within 7 days. Whereas other tools may take 12-18 months to build a baseline, MixMode is able to realize this industry-leading 7-day period through our AI's context-aware nature. We do not rely on statistical learning or static training data to form your baseline, but rather use the context of your own network to create the model upon which decisions are made.

Further, your baseline evolves with your network and provides the necessary context for the delivery of security alerts that are precise and actionable on an ongoing basis. The MixMode platform provides results that are actionable and tailored to your specific deployment. This means your team will begin seeing value within a week of deployment.

What is Third Wave AI and Why Should I Care?

Third wave AI, as described by the DoD and DARPA, is Artificial Intelligence that is able to adapt to changing situations that it has never seen before. This is different than first wave AI, which is essentially rule- or threshold- based machine learning. It is also different than second wave AI, which utilizes statistical training models in place of the aforementioned rules and thresholds. According to DARPA's former Director Dr. Steven Walker, waves one and two lack "contextual reasoning capabilities and their training must cover every eventuality, which is not only costly, but ultimately impossible."

This is the primary reason why third wave AI is critical for cybersecurity. Each corporate network is unique and is constantly changing. Only third wave AI can adapt to this dynamic use case and produce results that are accurate without the need for constant tuning.

The second reason that third wave AI is critical to your cybersecurity operation is it's unique ability to detect zero-day exploits and insider attacks. Most cybersecurity tools rely on intel-based alerting that is inherently historical. Intel is created once an attack is realized and diagnoses so by its very nature it is at best a history of attacks that have already taken place. Similarly, second-wave supervised learning AI systems make decisions based on static training data that is created by vendors and update sporadically. This means that it also is only good at seeing attacks that it has seen before. Neither of these systems will be able to detect a zero-day attack or an insider attack that is calculated to look like normal activity.

Third-wave unsupervised learning on the other hand is able to detect anomalies and attacks that have never been seen before due to its awareness of your specific network's behavior (not static training data).

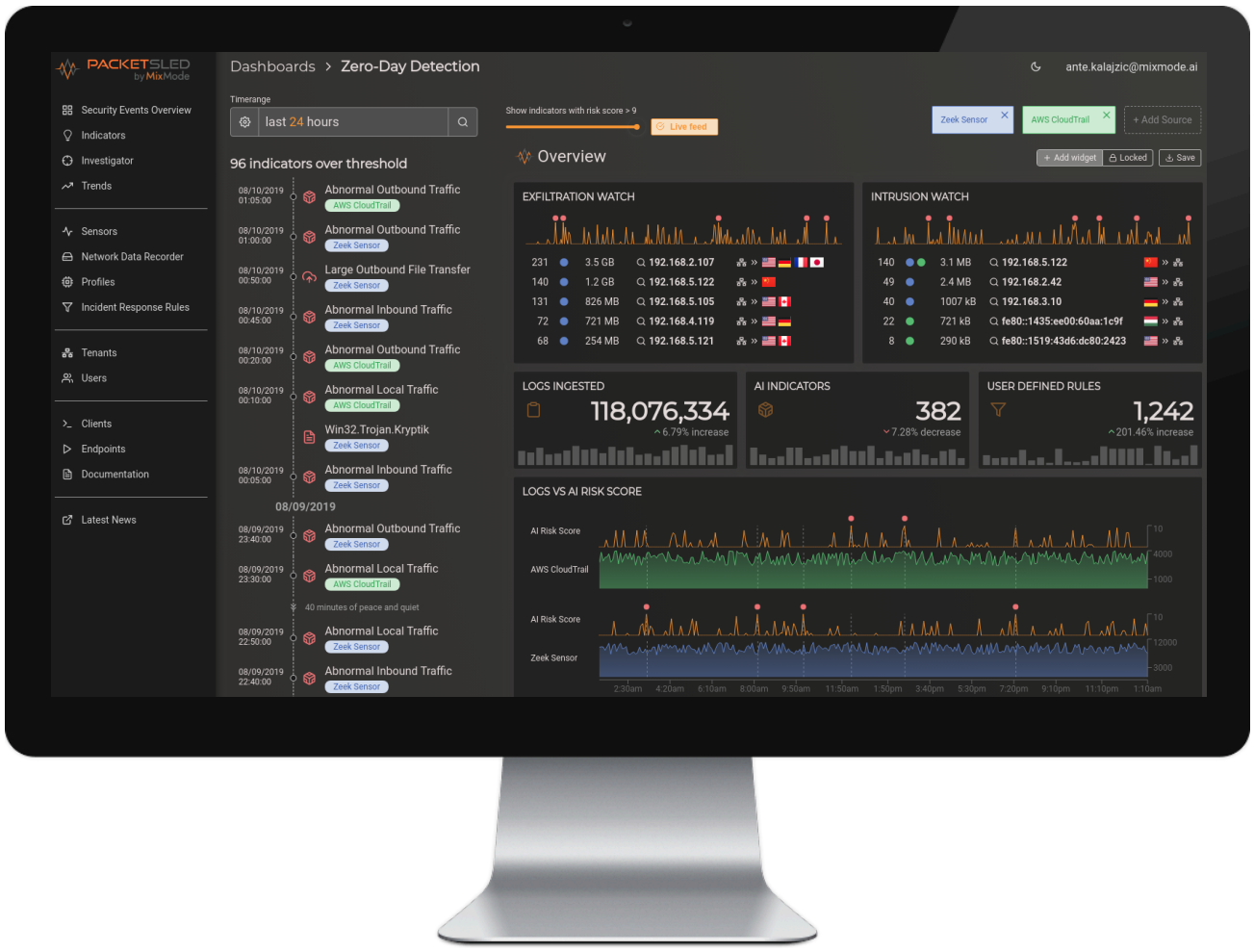
MixMode's AI Makes Your Data Actionable

MixMode created its purpose-built AI engine by leveraging algorithms that were fine-tuned over a twenty-year period of deployment for various DoD and DARPA projects. In adopting these AI algorithms, MixMode created a platform unlike anything else on the market - Third Wave Artificial Intelligence tailored to the specific challenge of cybersecurity and false positive alert reduction.

The power of MixMode's Artificial Intelligence lies in the fact it is learning from the behavior of your specific network.

Our experience has proven that most security engineers do not have a complete understanding of what is "normal" for their network as it contains an enormous amount of data to analyze. MixMode has solved this big data problem with its proprietary AI. Once a sensor is deployed, the AI engine analyzes various inputs around host- destination details and overall traffic behavior trends provided by network wire data, intel feeds and other private/public databases in real time.

For example, when analyzing your network wire data, MixMode considers factors such as the day/time, host/source/destination information, the size of traffic between given IPs, frequency of traffic between IPs, etc. to develop an understanding of what is the expected behavior for all of the IPs on your network.



This information is aggregated and processed through our proprietary AI engine and a predictive model or “baseline” of the "normal" behavior for your network is created. This is sometimes called a “generative model” as it is predicting the behavior of your network even if it has not seen similar behavior on it before. An initial baseline is produced in less than one hour, and this baseline is continually refined on an ongoing basis.

A complete baseline set is one seven-day week of data as the AI needs to learn what a standard week looks like. This allows us to consider the normal fluctuations in your business operations. For example, the normal working hours of 8:00 a.m. - 6:00 p.m. will create a baseline behavior pattern that is lower during the evening, begins increasing at 8:00 a.m., possibly dips at noon because of lunchtime, and drops back to a lower level at 6:00 p.m. Similarly, the AI is capable of recognizing the difference between a Monday at 3:00 p.m. and Friday at 3:00 as the behavior of employees and the volume of work product would likely differ. All of this is possible because of the third wave nature of MixMode’s AI.

Once a full baseline is achieved, our AI is capable of computing the standard fluctuation (i.e. fluctuation induced by normal human behavior on the network) from what is the predicted normal state of the network for a given timeframe.

This is done by comparing the current activities on the network with what is expected from the given timeframe. If the current network behavior deviates from the expected norm then alerting is enabled. If the current network behavior falls within a defined deviation of the expected norm, then alerting is suppressed. MixMode’s AI is purpose-built to handle large amounts of data and run on real-time traffic to ensure that your team is never overwhelmed with false-positive alerts.

The end result is that MixMode AI is able to consistently reduce the number of false positives for our clients by 90% or more versus rules-based systems. This mind-numbing exercise of combing through false positive alerts day after day is the kind of work that AI should be doing, so people can work on proactive and strategic problems facing their security teams.

The increase in the quality of the data your team is being asked to address will significantly reduce the burden of chasing false positives and decrease your risk posture by ensuring that your team is not ignoring alerts due to sheer volume.

Summary

In summary, MixMode’s AI analyzes the full fidelity of your traffic data, determines the normal state of your specific network (including the normal behavior of random fluctuations) and makes decisions based on that context. By looking for deviations from this complex baseline, it is not only capable of determining whether an alert is a false positive or not, but also reveals the baseline of the network itself, including recognition of subnetworks and daily/weekly/seasonal patterns, that can be useful in an operational context.

What’s more, MixMode is transparent about showing you the behavior models that are built including heat maps and graphs that the AI generates internally to model (predict) normal traffic behavior on a given network. MixMode also give you the control to “toggle” the AI on or off so you can rest-assured that you will never miss an alert.