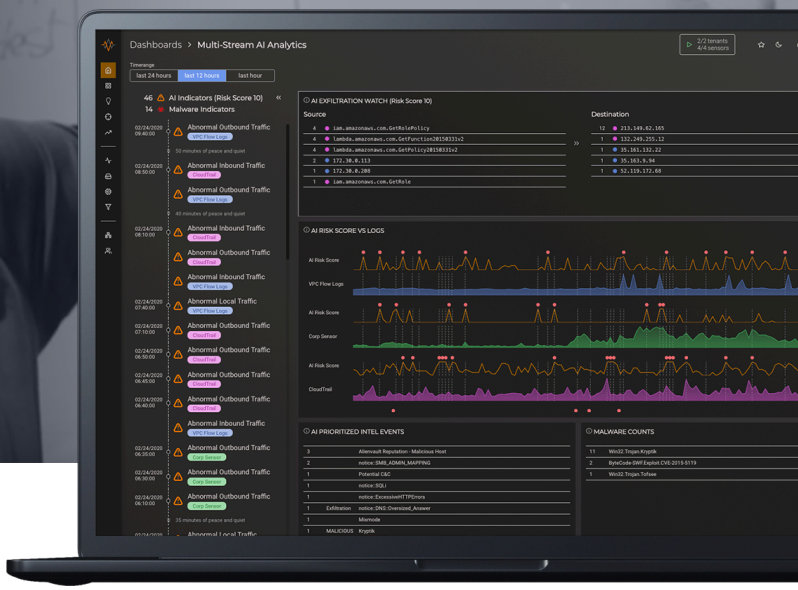
MixMode™

MIXMODE AI FREQUENTLY ASKED QUESTIONS



HOW IS THE AI PREDICTIVE?

MixMode's predictive capabilities work primarily two ways. First, our sensors detect anomalies that are breadcrumbs, or precursors to a breach. For example, it is able to detect beaconing intrusions that are precursors to a breach. Second, it is able to compare what it expects the network to look like on a specific date in the week/month and analyze traffic today against that.

YOU SAY YOU CAN ADDRESS ALERT VOLUMES. WHAT ABOUT FALSE NEGATIVES?

Mixmode's AI was built to analyze without human intervention the "health" of the network independent of any intel or notice feed. Our AI system improves the response by capturing anomalous events that are not captured by intel feeds. Thus, it minimizes BOTH the false positives AND the false negatives.

HOW DOES THE SYSTEM DIFFERENTIATE BETWEEN HIGH RISK ANOMALIES THAT GET A SCORE OF 10 AND LOW RISK ANOMALIES THAT GET A LOWER RISK SCORE?

MixMode's AI system constantly analyzes differentials between the observed behavior over the last 5 minutes and the behavior it expected to see in the last 5 minutes. The risk scores are based on computations of those analyses. Risk scores of 10 are indicators of severely abnormal behavior and thus need to be looked at with highest priority. Since MixMode's AI is constantly analyzing and comparing existing behavior against expected behavior, it is able to automatically adjust and categorize normal business spikes (e.g., spike in user volume associated with events like sales or seasonal behavior) as lower Risk anomalies. Customers have the ability to "tune" the focus on events that AI considers of lower priority, elevating the Risk scores for traffic the customer wants to designate as higher Risk.

HOW DO YOU DETECT ZERO DAY THREATS?

The algorithm underlying MixMode's AI is independent of any intel or notice feed. It captures anomalies that are predicated on behavior - an unusual behavior on the inbound pane that is not correlated to any alert from the intel feed might indicate an intrusion attempt that was not seen before, and thus might be a Zero-Day threat.

DOES THE AI LEARN WHEN THERE IS A CHANGE TO THE NETWORK (EX. A NEW PHONE SYSTEM IS PUT) IN OR DOES IT ALERT FOREVER ON THAT CHANGE?

If no action by the user is taken, the AI system will learn the new configuration.

DOES THE AI LEARN BY WATCHING WHAT THE OPERATORS DO WITH CERTAIN ALERTS -- WHETHER THEY REACT OR NOT SO THE AI KNOWS WHETHER TO FLAG IN THE FUTURE?

MixMode will be adding this capability to its platform in H2 2020

WHAT DOES "THIRD-WAVE AI" MEAN?

"Third Wave AI" is a term coined by DARPA and means artificial intelligence which can learn and adapt on it's own over time without the need for human training or tuning. Most security tools leverage first or second wave AI technology that use a combination of rules & thresholds or static "training" data to make decisions about your data. This technology can take between 6-24 months of learning to be effective. MixMode is the first Cybersecurity Platform to leverage true Third Wave AI in cybersecurity.

HOW IS YOUR AI "CONTEXT-AWARE"?

MixMode's AI analyzes all available underlying network data and feeds, taking into account the totality of the events on the network. Unlike second wave AI technology, MixMode's AI does not view events in isolation. MixMode's AI works to constantly analyze the expected traffic of an entire network against the behaviors taking place across a network every minute of every day. With each passing week, each day, each hour, each 5 minutes, MixMode's sensors are automatically analyzing network behavior against future behavior it has computed that it expects to see. Abnormalities are noted by risk scores within that full context

HOW MANY DAYS DOES IT TAKE TO TRAIN MIXMODE'S AI?

Unlike other human supervised cyber security systems, MixMode takes no human training and only 7 days to create a baseline of a network and start identifying anomalies.

HOW DOES MIXMODE'S AI DEFINE A THREAT?

MixMode's AI surfaces threats from analyses it makes about deviations from the normal behavior of a network; "normal" is generally computed from metadata and standard communication times, volumes and lengths of time.

CAN WE SEE ENCRYPTED TRAFFIC?

MixMode's AI assesses traffic volumes which include encrypted and unencrypted traffic. MixMode's AI does not need to decrypt traffic in order to analyze it.

HOW DOES THE BASELINE LEARN?

MixMode's AI utilizes a generative computational model. MixMode's AI constructs a denoised representation of the system over time by analyzing significant frequencies with which the system dynamics behave. MixMode's AI compares the current traffic volume to the denoised signal to determine if there are abnormalities in the current signal. This approach enables MixMode's AI to both flag anomalies within existing observed traffic as surface predictive and pre-attack behaviors on a network.

WHY DON'T YOU USE CLUSTERING TECHNOLOGY?

MixMode does not use clustering technology because networks are dynamic and utilizing clustering (like most vendors who claim to use unsupervised learning) for classification of anomalies are using an inherently flawed approach. Cybersecurity competitors utilizing clustering algorithms are unable to effectively analyze constantly changing network traffic patterns. These antiquated approaches and only allow for the discovery of structures within the dataset while not automatically labeling them. This means a user must still manually label those structures in order to ensure they are understood as abnormalities. This causes a need for constant updating, labeling, and tuning.

YOUR ALGORITHM IS UNSUPERVISED, SO YOU'RE JUST DOING CLUSTERING?

No. We build a generative model. This model can actually predict what the traffic will be in the next 5 minutes. Our algorithm is adaptable and can react to changing network conditions/topology, whereas clustering techniques are static and can't adapt to these changes. Additionally, the clustering algorithms such as K-means would still need an operator to go in and label which clusters represented normal traffic and attacks.

WHAT IF THERE IS CORRUPTED DATA DURING THE LEARNING PERIOD?

One should pay particular attention during the training period. If there is a risk score 10 interval it should be investigated. However, if no action is taken, if this corrupted data does not persist week to week, then the algorithm automatically adapts and the corrupted data is flushed from what is considered the normal baseline.

I HAVE A 5 MIN WINDOW THAT IS MARKED RISK SCORE 10. NOW WHAT?

Within that interval, all the intel and notices are available, in addition to all IP addresses that were active during that time. Also, the top three active IP's in that RISK 10 time interval are analyzed and labeled red if they showed unusual behavior, thus contributing to the root cause analysis.

WHAT DATA POINTS DOES THE AI USE TO MAKE A DECISION?

The AI looks at traffic flow between IP pairs in the network, splitting them into 3 directionalities; inbound, outbound, and lateral (internal to the network). The flows in each of these directions are used to build an adaptive, predictive baseline. Incoming traffic in a new 5 minute interval is compared to the expected behavior and a decision is made on whether it is anomalous or not.

WHAT HAPPENS IF THERE IS AN ATTACK DURING A LEARNING PERIOD?

During the initial learning period, attacks will still cause an AI alert to surface, but, due to the initial sensitivity of the AI algorithms, operators would need to be more vigilant during this period. However, the AI is adaptable. If this attack does not persist week to week, it will automatically be removed from the normal expected behavior of the network without operator supervision.

HOW FAR BACK DOES YOUR AI STORE DATA SO THAT IT CAN MAKE DETERMINATIONS ON CURRENT ANOMALIES?

The AI constructs a week-long baseline of normal behavior capturing all significant data structures in different periods within that week. Additionally this data is being updated with new data on a 5 minute period scale. Thus, at any given point in time, the AI provides a window into the last week of both normal and abnormal behavior of the network traffic volume storing only the relevant data for that span of time.

MORE QUESTIONS? CONTACT US!

Email info@mixmode.ai or Call (858) 225-2352. You can also send us a message at https://mixmode.ai/contact-us