MixMode™

MIXMODE AI FREQUENTLY ASKED QUESTIONS

HOW IS THE AI PREDICTIVE?

In two ways – one, the tech see anomalies that are breadcrumbs to a breach. for example, it can detect beaconing intrusions that are precursors to a breach. Second, it is predictive in that the system knows what a next thursday at 3pm will look like based on analysis of the previous times/days of the week.

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

Our AI is built as an assessment on the “health” of the network that is independent of any intel or notice feed. The 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 DO YOU DETECT ZERO DAY THREATS?

The algorithm underlying AI is independent of any intel or notice feed. It captures anomalies that are behavioral – 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.

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?

The AI system takes a differential between the observed behavior over the last 5 minutes and the behavior it expected to see in the last 5 minutes. The risk score 10 pertains to events that is severely abnormal and thus need to be looked at with highest priority. The user has the ability to “tune” the focus on events that AI considers of lower priority.

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.

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 uses a combination of rules & thresholds or static "training" data to make decisions about your data and 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"?

The AI takes in all the underlying network data and feeds that are available, and thus takes into account the totality of the events on the network, rather than viewing events on it in isolation. Thus, it is aware of the full context, e.g. the specific set of events that are expected to appear on the network on a typical Thursday at 11AM , and renders its judgement on the (ab)normalcy of an individual event in that full context.

HOW MANY DAYS DOES IT TAKE TO TRAIN THE MIXMODE AI SYSTEM?

Unlike other Supervised Cyber AI systems, MixMode takes no human training and takes only 7 days to create a baseline of a network and start identifying anomalies.

HOW DOES THE AI DEFINE A THREAT?

It is a deviation from the normal behavior of the network; normal is generally defined by metadata and standard communication times, volumes and lengths of time historically.

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