451 Research

S&P Global
Market Intelligence

Coverage Initiation: MixMode harnesses self-supervised AI to optimize threat detection and response

Analysts - Scott Crawford

Publication date: Friday, June 30 2023

Introduction

The theme of AI in cybersecurity has become more pronounced in recent months, but the substantial buzz around generative AI applied to security is still in its early stages. The need to apply innovation to improving threat detection and response is great. On average, respondents to 451 Research's Voice of the Enterprise: Information Security, Security Operations 2022 study that are using security analytics said they are unable to investigate nearly half (48%) of their security alerts on a typical day. This leaves too many blind spots and missed opportunities to act against a constant barrage of both current and emerging threats.

MixMode believes it has an answer to this ongoing problem through its cybersecurity platform that leverages a dynamic threat detection foundation model and use of self-supervised AI to deliver threat detection and response — an approach introduced prior to much of the recent buzz surrounding generative AI. Such an approach is likely to give security teams an edge over earlier rules-based or machine-learning-based analytics — capitalizing on the current generation of innovation to understand and respond much more quickly and effectively to a much larger volume and variety of inputs, including previously unseen evidence or complex threat patterns, without human supervision.

The Take

Unlike recent introductions that seek to capitalize on generative AI by using large language models for natural language search in security platforms, the MixMode AI model is more directly applied to threat detection. MixMode uses a dynamic threat detection foundational model that provides the ability to learn, adapt, predict and detect threats in any security environment. This enables the MixMode platform to identify new evidence indicating novel threats or previously unrecognized threat activity, without supervision or prior training. This also means it can potentially handle a much greater volume and variety of enterprise security data than many prior techniques. It can draw its own inferences, make its own correlations and ascertain baselines on its own to identify anomalies with a minimum of human effort. In this respect, MixMode could serve as a bellwether for the more direct application of AI in threat detection and response, across a large diversity of data sources at enterprise scale.

Context

Founded in 2020 with headquarters in Santa Barbara, Calif., MixMode sees its primary innovation as capitalizing in cybersecurity on what the US Defense Advanced Research Projects Agency (DARPA) has described as the "third wave" of AI. In this view, the first wave of AI used in security analytics relied on rules-based systems, identifying threat patterns based on human-defined criteria. Later innovations, referred to in this same frame of reference as "second wave AI," introduced statistically oriented machine-learning techniques to accelerate anomaly recognition. Often, however, such initiatives required human supervision to define the terms of analysis and maintain focus. "Third wave" innovation, as applied by MixMode, uses a dynamic threat detection foundational model that is self-supervised in its learning and can ingest and respond to inputs without direct human intervention. It can draw its own logical inferences and understanding of context.

This opens the door to many possibilities for enterprise security analytics. The speed and scale of such models should make larger volumes and a greater variety of data more actionable. Less "conditioning" of inputs may also be required, which can further reduce burdens for the data ingest and normalization often needed to give structure to data for analysis. They introduce the potential for identifying novel attacks and threat patterns previously unrecognized by human analysts or legacy models, such as rules-based detection, and to do so much more quickly. The efficiency of such AI models may also reduce both false positives and false negatives, improving the quality of actions resulting from findings. MixMode further claims that these capabilities can also reduce storage costs relative to more traditional platforms.

MixMode has so far raised $62 million in funding, most recently in a $45 million series B in March led by PSG. Co-founders John Keister and Igor Mezic lead the company as CEO and chief scientist, respectively. In the face of a challenging economic climate, the company indicates it has more than doubled its number of employees over the prior year.

Technology and products

Deployed as SaaS and taking inputs from a variety of sources, from cloud providers as well as on-premises tools, MixMode exposes its benefits to security teams as a dynamic detection layer for security operations, through three primary interfaces of the product: Alerting, Investigation and Reporting.

The Alerting function is typically the initial interface encountered by security analysts. It displays specific alerts based on the recognition of malicious patterns by the AI model, in terminology recognizable to security teams. Detailed explanation of detected events is available, as well as remediation actions and reference to MITRE ATT&CK definitions. Filtering options allow analysts to categorize and assign alerts; view alerts by a number of criteria, such as host or detection type; and enable ticketing for response workflows. The AI model is self-normalizing, meaning that no training data is required to "prime" the threat detection functionality, nor are any human-defined rules or thresholds required. Instead, the model learns to recognize significant events in the body of data available, which also enables it to apply and improve self-determined noise reduction to surface the most significant issues for analyst teams.

When events warrant, the Investigation function supports more detailed triage and deeper analysis. Drill-down, such as raw log data, is available to support more in-depth analysis. The Reporting function supports SecOps teams with data on ingestion, bandwidth statistics and other parameters to support operational requirements. Capping the user experience is a Dashboard function that provides high-level analytics and data visualizations, such as frequency of detections and distribution of detections by type, entity, geographic location and other parameters.

Competition

MixMode is one of a growing number of vendors in evolving security operations architectures, which has broadened to include multiple aspects of detective analytics, response functionality, data aggregation and management, and the functionality necessary to integrate across these domains. MixMode competes most directly in threat detection, investigation and response, where competitors include the likes of Arista (through its acquisition of Awake Security), Cisco Systems Inc.'s Secure Network Analytics (formerly Stealthwatch), Corelight, Darktrace PLC, ExtraHop, Gigamon, Netography, Vectra AI and others with a primary focus on the detection of threats in networks. In this respect, they often complement other SecOps technologies, such as security information and event management. Many vendors in multiple aspects of SecOps have embraced AI and machine learning in a variety of ways, including more recent innovations; those that have emphasized AI functionality as a primary differentiator in its own right include StrikeReady in SecOps tech, as well as Expel's "bots" in managed detection and response.

As the race to make the most of generative AI in virtually every aspect of technology continues to heat up, cybersecurity can be expected to be a focus of innovation. Indeed, two of the largest vendors not only in IT, but also in SecOps tech, Microsoft Corp. and Google, each introduced its own initial generative AI concepts for security operations teams shortly before or at the 2023 RSA Conference in the US. A host of other vendors have joined in to capitalize on the buzz and make much of the opportunity. MixMode will need to demonstrate its differentiation in actionable threat recognition and response against what seems poised to become a very noisy field.

SWOT Analysis

Strengths	**Weaknesses**
While others — including some of technology's largest players — have only recently come to the generative AI party in cybersecurity, MixMode has been investing in dynamic threat detection using third wave AI (as defined by DARPA) since its inception. This gives it a track record in AI application to threat recognition from enterprise-scale input volume and variety ahead of some of its most significant competitors.	As an emerging startup, MixMode may face constraints in resources and opportunity compared with some of its largest competitors. The advantage of the opportunity at present is that the need is great, and the market's receptivity to improving the efficacy of threat detection and response is high.
Opportunities	**Threats**
The need to optimize threat detection and response from overwhelming data has plagued security operations for years. The capabilities of emerging AI seem poised to harness the promise of varied, large-scale data in ways previously inaccessible to prior technologies.	The largest vendors not only in technology but in security operations are also major investors in the evolution of AI. MixMode will have to demonstrate continued differentiation in the actionability of its offering to resonate with prospects that must now separate fact from noise in the race to make the most of the AI moment.

Source: 451 Research.