MixMode®

UTILIZING ARTIFICIAL INTELLIGENCE EFFECTIVELY IN CYBERSECURITY

Comparing the Pros and Cons of Various AI Approaches in Cybersecurity

www.mixmode.ai | +1 (858) 225-2352 | info@mixmode.ai |

OVERVIEW

Artificial intelligence (AI) has revolutionized cybersecurity by enabling a more proactive and adaptive approach to defend against ever-evolving cyber threats. AI technologies like machine learning, natural language processing, and intelligent automation are addressing critical security challenges, including:

- **Detecting advanced threats**
  AI analyzes massive data volumes from networks, endpoints, cloud, etc., to detect emerging anomalies, malware, malicious behaviors, and other risks that evade rules-based systems.
- **Accelerating threat response**
  AI automates tedious aspects of security workflows, provides context for alerts, and orchestrates containment of attacks to enable faster reaction.
- **Amplifying analyst capabilities**
  AI augmentation features like virtual assistants free analysts to focus on higher-value efforts and make informed decisions faster.
- **Predicting and simulating new attacks**
  Advanced AI-like generative models can forecast attacks based on curated threat intelligence and synthesize realistic threat scenarios for defense testing.
- **Securing cloud environments**
  AI applied directly in cloud platforms provides enhanced visibility, behavioral monitoring, and threat detection as assets migrate to the cloud.
- **Strengthening identity management**
  User behavior analytics and risk scoring driven by AI help defend against compromised credentials, account takeover, and insider threats.

AI is becoming indispensable for maintaining strong defenses as cyber risks grow, but it must complement human expertise. The optimal cybersecurity strategy combines AI's speed and scalability with analyst judgment and oversight.

Several AI approaches are used in cybersecurity, but it's hard to make sense of the noise, especially when vendors say the same thing.

In this eBook, we'll explore what they are and the pros and cons of each one.

COMPARING THE PROS AND CONS

Machine Learning (ML)

Machine Learning is not AI but has been included here since it's been lumped into the AI conversation and should be considered a stepping stone to true artificial intelligence in cybersecurity solutions.

Machine learning algorithms analyze large volumes of data to identify patterns, anomalies, and indicators of malicious activity. ML models are trained on historical data to make predictions and decisions based on new or unseen data.

How it's used: Built into many security tools to help automate identifying security incidents and threats, analyzing them, and in some cases, automatically responding.

PROS

- Speeds up the threat detection process.
- Uncovers malicious activity.
- Automates remedial, mundane, and transactional tasks that burden technical roles.

CONS

- Expensive to implement and maintain.
- Difficult to explain how machine learning models make decisions.
- Difficult to ensure that machine learning models are not biased.

Deep Learning

Deep learning is a subset of machine learning that uses neural networks with multiple layers to learn complex patterns and representations. Deep learning models excel at tasks such as image recognition, natural language processing, and behavior analysis.

How it's used: It enhances threat detection accuracy, speeds up response times, and provides proactive defense against sophisticated attacks.

PROS

- Solves complex problems quickly.
- Automates many tasks.
- Identifies complex interactions.

CONS

- Computationally intensive.
- Requires abundant data.
- Can be opaque, meaning it can be challenging to explain how deep learning models make decisions.

COMPARING THE PROS AND CONS

Natural Language Processing (NLP)

NLP focuses on understanding and processing human language. It enables the analysis of textual data, such as security logs, threat intelligence, and user communications, to extract meaningful insights and identify potential threats.

How it's used: Can be leveraged in cybersecurity workflows to assist in breach protection, identification, and scale and scope analysis.

PROS

- Identifies overlaps in standards and frameworks, data from an organization's tech stack, and threat feeds to identify vulnerabilities in your security infrastructure.
- Detects phishing activity and malware through keyword extraction in email domains and messages.

CONS

- Can raise concerns over privacy, accuracy, and fairness.
- Some models are often trained in imperfect datasets, which produce problematic outcomes.
- Models can also need help with context and meaning, which leads to misinterpretation and miscommunication.

Behavioral Analytics

Behavioral analytics uses AI techniques to establish normal user and system behavior baselines. Deviations from these baselines can indicate malicious activities or insider threats. AI-powered behavioral analytics systems continuously monitor for unusual behavior and trigger alerts or take automated actions when anomalies are detected.

How it's used: Analyzing user behavior patterns and identifying anomalies that may indicate a security breach.

PROS

- Can help detect more sophisticated threats.
- Makes security tools more flexible.
- Uncovers data theft and other insider threats.

CONS

- Generates a lot of false positives, which can be time-consuming for security teams to investigate.
- Requires collecting data on users' behavior, which can raise privacy concerns.
- Complex and challenging to implement.

COMPARING THE PROS AND CONS

Reinforcement Learning

Reinforcement learning is an AI approach where an agent learns to make decisions based on trial-and-error interactions with an environment. It involves training an algorithm to make decisions based on rewards and punishments.

How's it used: Can be used to optimize security controls, automate response actions, or improve threat-hunting strategies.

PROS

- Can help detect and prevent cyberattacks.
- Identifies patterns in data that other methods might miss.
- Automates manual security tasks.

CONS

- Too much reinforcement may cause an overload which could weaken the results.
- Reinforcement learning is preferred for solving complex problems, not simple ones.
- Requires lots of data and processing power.
- Maintenance cost is high.

Generative AI

Generative AI models can create new data samples or simulate realistic scenarios. In cybersecurity, generative models can generate synthetic data for training purposes or simulate potential attack vectors to evaluate system defenses.

How it's used: Create synthetic data that can be used to simulate cyber attacks and test the effectiveness of security systems.

PROS

- Simulates attacks to help strengthen infrastructure.
- Assists with testing security defenses.
- Facilitates a shift away from a defensive stance to a proactive stance.

CONS

- Can expose organizations to new attack vectors and security risks.
- Difficult to distinguish between normal and abnormal behavior.
- Need help understanding and interpreting the results.
- Expensive to implement.

LARGE LANGUAGE MODELS

One type of Generative AI leverages large language models (LLMs) to generate novel combinations of text in the form of natural-sounding language. LLMs are one type of generative AI since they generate other outputs, such as new images, audio, and even video.

LLMs are trained on a massive trove of articles, Wikipedia entries, books, internet-based resources, and other input to produce human-like responses to natural language queries. They are a type of AI currently trained through data input/output sets; frequently, the text is unlabeled or uncategorized, and the model uses self-supervised or semi-supervised learning methodology.

A large language model (LLM) is an artificial intelligence system trained on massive volumes of text data to understand and generate natural language. The key aspects of large language models are:

- **Size**
  They are trained on billions or trillions of words from books, websites, code, and other text sources. The vast dataset enables them to learn nuances of human language.
- **Architecture**
  They use deep learning neural networks with transformer architectures. The transformer enables modeling longer-range dependencies in text.
- **Representation**
  They develop high-dimensional vector representations of words, sentences, and documents that capture semantic meaning and relationships.
- **Generation**
  Besides analyzing language, LLMs can generate new coherent, human-sounding text for a given prompt or task.
- **Scaling laws**
  As LLMs are scaled up, they display a power law improvement in capabilities like reasoning, knowledge representation, and language fluency.
- **Self-supervision**
  Many recent LLMs are trained using self-supervision, learning by predicting masked words rather than needing labeled data.

Examples of large language models are GPT-3, Turing-NLG, Jurassic-1, and LaMDA. Their advanced language understanding and generation abilities enable applications across search, translation, writing assistance, and more.

LARGE LANGUAGE MODELS

Large language models (LLMs) have been used for threat detection in various ways, including natural-language-based threat hunting, categorization, and more precise explanations of complex malware.

However, there are also some downsides to using large language models for threat detection, particularly in the cloud, since training and deployment of LLMs require extensive computing resources and data storage.

POTENTIAL PROS

- Understand nuanced language in logs, packets, and alerts to extract indicators and behaviors
- Generate realistic phishing emails and malware source code for training and testing
- Summarize long security documents and alerts into concise insights
- Ability to process vast volumes of unstructured text data
- Answer analyst questions with detailed contextual explanations
- Continually improve by training on new data without manual retraining
- Automate repetitive tasks like triage to reduce analyst workloads
- Adapt quickly to new types of textual threats and attack tactics
- Leverage massive threat intelligence data to forecast emerging techniques

POTENTIAL CONS

- Could automate the production of convincing malicious content
- Lack of explainability compared to other AI techniques
- Require extensive computational resources for training and inference
- Potential for bias, toxicity, and errors in training data
- Not optimized specifically for security tasks out of the box
- Overreliance could cause oversights of threats not detectable in text
- Adversarial manipulation of text could degrade model accuracy
- Malicious actors could leverage models for attacks
- An accelerated arms race in generative AI between attackers and defenders

COMPARING THE PROS AND CONS

Dynamical Systems Foundational Model

The Dynamical System Foundational Model (DSFM) is based on the principles of dynamical systems theory, which studies how systems evolve and how internal and external factors influence their behavior. In cybersecurity, the DSFM considers the dynamic nature of security environments and the interconnectedness of various components within a system.

How it's used: It can help detect and respond to threats by rapidly mining large amounts of data, processing many signals, identifying anomalies, and developing predictions.

PROS

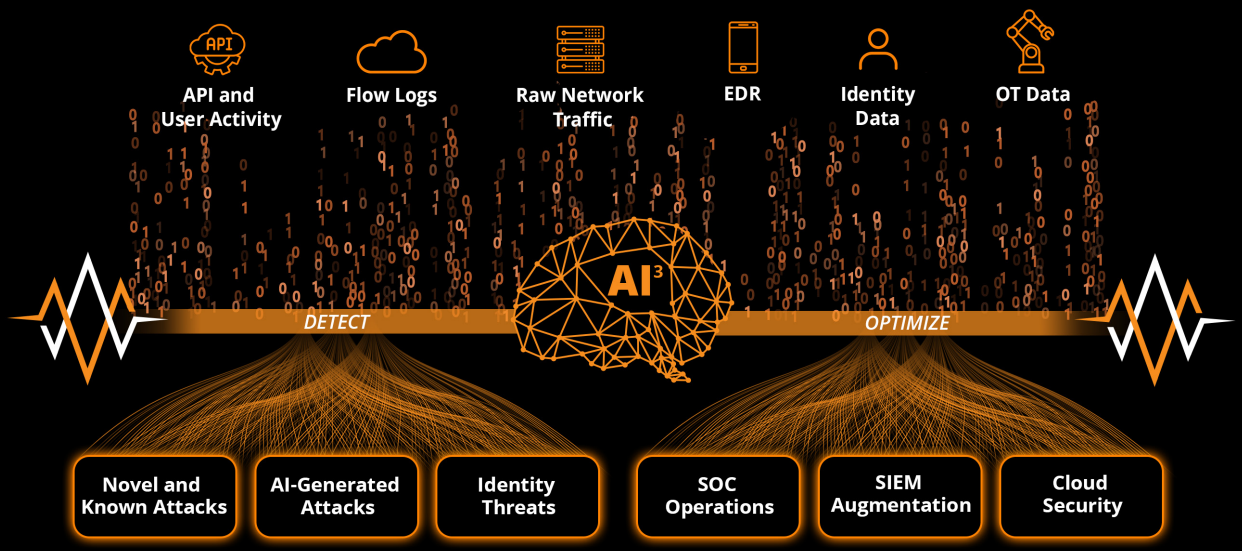
- Capable of scaling and analyzing large data sets.
- Can be used to identify patterns in data that can identify threats in real-time.
- Can adapt and evolve with the threat landscape.

CONS

- Often confused with Generative AI LLM.

MixMode's Generative AI

A generative model purpose-built for threat detection and response is needed for true detection and response. MixMode's generative AI is uniquely born out of dynamical systems (a branch of applied mathematics) and self-learns an environment without rules or training data. MixMode's AI constantly adapts itself to the specific dynamics of an individual network rather than using the rigid legacy ML models typically found in other cybersecurity solutions.



CONCLUSION

Like it or not, artificial intelligence is fundamentally transforming cybersecurity and has only begun scratching the surface of its potential.

As models are trained on ever-growing datasets, AI will continue developing new levels of sophistication and intuition in areas like adversarial content generation, data correlation, pattern recognition, and predictive risk analysis.

However, human expertise must continue guiding cybersecurity strategy. AI should augment and enhance human capabilities, only partially replace their tasks. By combining the complementary strengths of human insight and AI, cybersecurity teams can ensure their organizations are well protected.

The future remains unclear, but one thing is sure - AI will be the driving force that redefines cyber defense as we know it. **Organizations must adopt AI proactively to be resilient in the face of what's to come.**

MIXMODE OVERVIEW

The Mixmode Platform augments key capabilities found in SIEMS, UEBA, NDR, and other cybersecurity solutions, eliminating the need for multiple disparate toolsets. The MixMode Platform assimilates and evolves with an organization's infrastructure to provide real-time threat detection and response across cloud, hybrid, and on-prem environments through:

Network Traffic Analysis: Captures and examines network communications, including the flow of data packets, to detect anomalies, identify potential security threats, and gain comprehensive visibility into all network operations.

Behavioral Analysis: Analyze the behavior and activities of users, systems, and entities within a network or system to detect anomalies and potential security threats.

Advanced Threat Detection: Recognize patterns of behavior that may indicate a cyber attack to help cybersecurity teams detect threats that would otherwise go unnoticed or bypass traditional security tools.

Predictive Analytics: Analyze large amounts of data to identify potential threats and predict future attacks to help cybersecurity teams stay ahead of threat actors and take proactive measures to protect their organizations.

Real-time Monitoring: Ingest, correlate, and analyze large data sets in real-time to fully protect the entire infrastructure of an enterprise organization.

No rules. No tuning. No maintenance. Any environment.

Cloud Native | On-Prem | Hybrid

MixMode is the leader in delivering generative AI cybersecurity solutions at scale. MixMode offers a patented, self-learning Platform designed to detect known and unknown threats in real-time across cloud, hybrid, or on-prem environments. Large enterprises with big data environments, including global entities in financial services, fortune 1K commercial enterprises, critical infrastructure, and government sectors, trust MixMode to protect their most critical assets. Backed by PSG and Entrada Ventures, the company is headquartered in Santa Barbara, CA. Learn more at www.mixmode.ai.

www.mixmode.ai | +1 (858) 225-2352 | info@mixmode.ai |