AI DETECTION IN CYBERSECURITY

Foundational Models can be applied to various aspects of cybersecurity. Here's how:

LEGACY RULES

The basic rules model in cybersecurity refers to a traditional approach where predefined rules and signatures are used to analyze and detect threats.

MACHINE LEARNING

In cybersecurity, a Machine Learning (ML) model is a computational algorithm that uses statistical techniques to analyze and interpret data to make predictions or decisions related to security.

LARGE LANGUAGE MODELS

Large Language Models (LLM's) are trained on data to allow for intuitive search and automation when analyzing data in cybersecurity environments.

DYNAMICAL SYSTEMS

The Dynamical System Foundational Model (DSFM) is used in cybersecurity to model and analyze complex systems, such as network infrastructures or software applications, to identify vulnerabilities, detect threats, and mitigate risks.

LEGACY RULES

This process typically involves creating rules based on known patterns and indicators of cyber threats. These rules can be designed to detect specific types of attacks, such as malware signatures, known vulnerabilities, or suspicious network behavior. The model is then utilized to process and analyze security logs, network traffic, and other relevant data, helping to identify potential threats based on the predefined rules.

While this approach can effectively detect known threats, it has limitations when identifying new or evolving threats.

EXAMPLES exabeam LogRhythm securonix sumo logic corelight

KEY INSIGHTS

- Needs to be continuously updated and expanded to keep pace with emerging attack techniques.
- Struggles to handle complex or contextual nuances in cybersecurity, as it relies on predefined patterns rather than adaptive learning.
- Lack of transparency makes it difficult to explain the reasoning behind their decisions or identify biases in their outputs.

MACHINE LEARNING

ML models are trained on large datasets that include normal and malicious behavior, enabling them to learn patterns and identify anomalies that may indicate potential threats.

ML models can be applied to various use cases, including threat detection, malware analysis, user behavior analytics, and vulnerability management.

EXAMPLES VECTRA DARKTRACE ExtraHop

KEY INSIGHTS

- Requires ongoing monitoring, updating, and refinement to adapt to emerging threats and changes in the security landscape.
- Continuous evaluation and improvement of ML models are essential to maintain their effectiveness.
- Susceptible to adversarial attacks, where malicious actors manipulate input data to deceive the model and evade detection.

LARGE LANGUAGE MODELS

Large language models are trained on huge datasets to generate human-like text and understand natural language queries; their natural language capabilities allow more intuitive search and automation when dealing with unstructured data in cybersecurity.

Large Language Models are transformer-based models which have impressive language generation capabilities enabling advanced conversation and text generation, and includes tools like ChatGPT.

Large language models are trained on huge datasets to generate human-like text and understand natural language queries; their natural language capabilities allow more intuitive search and automation when dealing with unstructured data in cybersecurity.

EXAMPLES SentinelOne Google Microsoft

KEY INSIGHTS

- LLMs excel at natural language search because their broad training enables interpreting free-form queries and unstructured data like logs and reports.
- LLMs struggle with detection because they lack contextual awareness and reasoning abilities to deeply analyze relationships and make sound judgements.

DYNAMICAL SYSTEMS

The 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.

EXAMPLE

MixMode®

KEY INSIGHTS

- Enables real-time threat detection and response for known and unknown attacks.
- Provides a comprehensive and adaptable framework for managing and securing enterprise environments.
- Facilitates proactive risk assessment, early detection of threats, and timely response to security incidents.
- Understands network dynamics to implement effective security measures and enhance their overall cybersecurity posture.
- Does not require large training data sets or human tuning and maintenance of the model unlike other models.

THE FOUNDATIONAL AI MODELS APPLIED TO CYBERSECURITY

AI-driven solutions are becoming increasingly important in detecting sophisticated threats. But not all AI based cybersecurity solutions are the same. Most solutions are utilizing Legacy Rules and Machine Learning models, relying on rules-based approaches that can only detect attacks with known signatures and cannot effectively scale.

MixMode has developed the world's first commercially available intuitive threat detection and response platform built on Dynamical Systems AI. MixMode's patented self-learning AI platform identifies patterns and trends without predefined rules or training. **Learn more: mixmode.ai/ai/**