Innovation Unleashed: **The Disruptive Force of Predictive AI on the Cybersecurity Industry**

Whitepaper

2023

AGILEBLUE

INTRODUCTION

In today's rapidly evolving digital landscape, the cybersecurity industry finds itself facing a formidable adversary – cyber threats of unprecedented complexity and sophistication. As organizations strive to fortify their defenses and safeguard sensitive data, a groundbreaking force has emerged to revolutionize the way we approach security challenges: Predictive AI. Powered by cutting-edge machine learning algorithms, predictive AI has proven to be a game-changer, empowering cybersecurity professionals with unparalleled capabilities to proactively anticipate, detect, and mitigate cyber threats before they materialize. In this white paper, we will discuss how predictive AI is disrupting the cybersecurity industry, reshaping the way we defend against cyberattacks, and paving the way for our society's digital future.

As the landscape of cybersecurity advances and malicious actors grow more sophisticated, organizations must adapt accordingly. To safeguard against the next generation of hacks and breaches and maintain a robust cybersecurity posture, security teams must adopt a proactive approach to Network Traffic Analysis (NTA). Current industry solutions often rely on artificial intelligence models that suffer from a fundamental flaw – they compare network behavior solely against a historical baseline analysis, which is formed after months of data aggregation, storage, and analysis.

To effectively combat the ever-evolving threats posed by new malicious actors and attacks, it is crucial to have an accurate, forward-looking, and continuously evolving baseline of "normal" network behavior. Traditional cybersecurity solutions claiming to provide anomaly detection through AI encounter a significant issue: their baselines are solely based on historical data that takes months to gather, leading to an increase in false positives and an inability to adapt to evolving network conditions and attacker tactics.

Predictive vs. Generative AI

Predictive AI and generative AI represent two distinct paradigms within the broader field of artificial intelligence, each serving unique purposes and employing different methodologies.

Predictive AI, also known as supervised learning, is a type of AI that focuses on making predictions based on existing data patterns. It is designed to learn from historical data with labeled outcomes, enabling it to recognize patterns and correlations. By training on past examples, predictive AI can predict future outcomes when presented with new data points. However, its predictive capabilities are limited to what it has been explicitly trained for, and it lacks the ability to generate entirely novel content or data.

On the other hand, generative AI operates under unsupervised learning, aiming to create new content or data rather than predicting predefined outcomes. This type of AI is capable of generating original and creative outputs by identifying underlying patterns and structures within the input data. While generative AI showcases tremendous creativity and innovation, it lacks the focused predictability of its predictive AI counterpart.

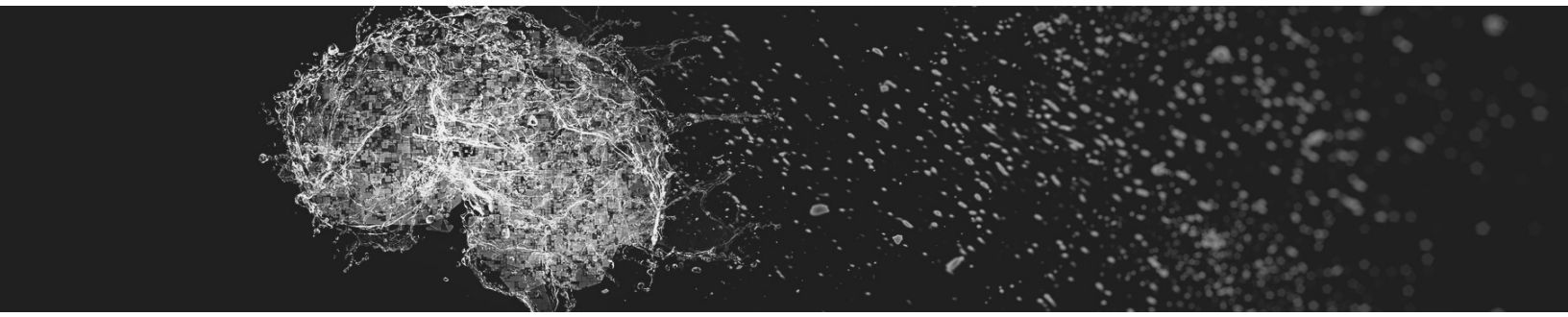
Advancing Past First- and Second-Wave AI

Compared to third-wave context-aware solutions, first and second-wave AI implementations prove significantly less effective. To grasp the constraints of early AI-enhanced security solutions, we must first explore the motivations behind the development of these initial AI functions.

First-wave AI introduces automation to repetitive and narrowly defined tasks. This type of AI is designed for specific problem-solving purposes and relies solely on human inputs related to the targeted issue. While the advent of first-wave AI marked a significant advancement in technology, it becomes apparent that its security capabilities are inadequate for sprawling, distributed networks.

Second-wave AI demonstrates improved classification and prediction capabilities, yet its reasoning capacity remains limited. SIEM cybersecurity platforms are a prevalent example of second-wave AI applications in modern times. Although these platforms often incorporate automated features and some unsupervised behavior, they heavily rely on continuous human interaction, tuning, configuration, and guidance to operate effectively.

Third-wave AI platforms are characterized by their context-awareness and utilize a generative model stemming from self-supervised learning, enabling them to transcend the mere identification of unusual activities and delve into the realm of predicting future outcomes.



PREDICTIVE AI USES IN CYBERSECURITY

Threat Monitoring Automation

To effectively monitor threats to your network, you will need to sift through vast amounts of both unstructured and structured data. Doing this manually can be time-consuming, and even with a team of people, there is still a risk of overlooking significant data points. Fortunately, you have the option to automate the threat monitoring process using predictive AI. By leveraging predictive AI, you can eliminate human errors and achieve a more cost-effective approach in the long run compared to manual data checks. Moreover, predictive AI empowers you to enhance your company's model and risk management, thereby reducing the likelihood of cyber-attacks and ransomware incidents, or at the very least, significantly mitigating the damage and losses they may cause.

Improved Risk Management & Incident Response

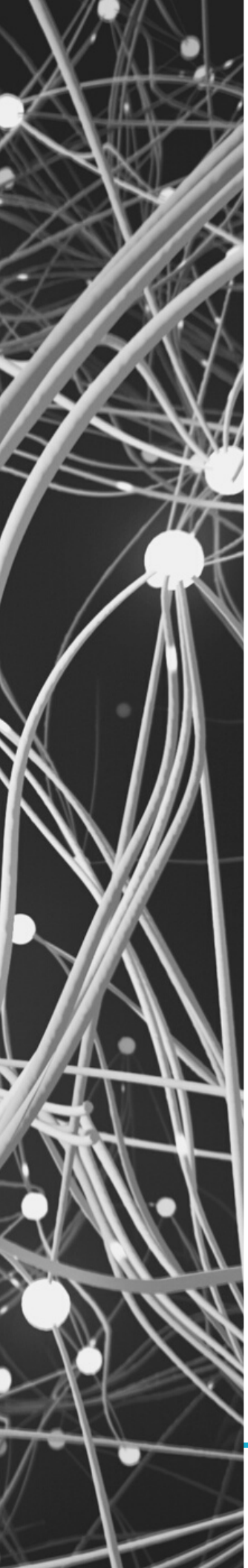
With predictive artificial intelligence at your disposal, you can efficiently analyze vast amounts of collected data to make informed decisions when confronting imminent threats.
This enhanced predictive analysis approach empowers you to make data-driven choices and gain valuable cybersecurity insights, which prove instrumental in strategic decision-making and selecting the appropriate incident response measures. Furthermore, these advanced cybersecurity policies can be seamlessly integrated into your handling of third-party services, fortifying your defenses and preventing potential data breaches.

Sensing Cyber Risks

The primary advantage of employing predictive AI in cybersecurity lies in its remarkably advanced risk sensing and prediction capabilities, outperforming human manual checks and rigid rule-based algorithms with unparalleled efficiency. Leveraging its self-learning capacities, predictive AI facilitates a highly efficient process that allows companies to detect new anomalies, evaluate associated risks, and generate future risk predictions.

Preventing Cyber Crime

By adopting predictive AI, you can effortlessly maintain comprehensive 24/7 protection that surpasses human cybersecurity interventions. With its predictive abilities, third-wave AI can promptly alert you about zero-day vulnerabilities in your company's software even before a breach occurs. These vulnerabilities can be exploited by hackers through zero-day attacks, utilizing exploits to gain unauthorized access to your system and compromise its security.



KEY SOC ISSUES THAT IMPACT NETWORK TRAFFIC ANALYSIS

1. The Wasteful Culture of False Positives and the Wasted Potential of Security Analysts

There is a significant challenge faced by organizations due to the substantial number of false positive alerts triggered by SIEM platforms. This issue not only consumes valuable time and human resources but also exposes organizations to increased vulnerabilities, setting off a chain of security events. The opportunity cost of allocating resources to handle false positives may result in serious network breaches occurring in the meantime.

According to a recent report from the Ponemon Institute, the typical organization wastes between 286 and 424 hours each week dealing with false positives. The time spent hunting down these threats emerges as one of the primary factors contributing to the ineffectiveness of security operations centers (SOCs), as reported in the study. In fact, 49 percent of companies cite false positives as a top challenge,

- Up to 25% of a security analyst's time is dedicated to pursuing false positives, meaning that approximately 15 minutes of each working hour is expended on unproductive threat hunting.
- Enterprises waste 21,000 hours and spend $1.3 million annually dealing with false positives

2. The Factor of Human Error

Due to the human factor of analysts, SOC and CISO managers anticipate a certain level of human error throughout security procedures.

- A recent Kaspersky Lab report presents a comparable statistic concerning cloud-based data breaches, attributing 90 percent of these breaches to employees themselves, resulting in a corporate cost ranging from $1.25 million to $8.19 million each.

Whenever humans interact with technology, the potential for errors arises. The connection between SIEM and human interaction is undeniable. A SIEM platform's capabilities are confined to the data stored in a system, and that data is inherently influenced by human actions. From configuring firewalls to setting access controls and determining the severity of threats to address, these decisions are all based on network data and human input. In reality, the network's behavior in response to human interaction provides much more comprehensive and accurate insights for risk assessment.

Automate your Cybersecurity With the Right AI

Our Cerulean platform gives you the power of AI-based automation with the support of a dedicated team. Our team of cyber experts are always available 24/7 to offer guidance and response, ensuring that you can get the most out of your automated intelligence cybersecurity platform. Our autonomous platform provides a smarter way to protect your business, allowing you to focus on the big picture and sleep at night!

Collect & Analyze
Our platform collects, analyzes, and correlates data from every digital asset. Using machine learning algorithms, AgileBlue can detect anomalous activity and prioritize alerts based on the severity of the threat with the appropriate response to mitigate risk.

Automate
When a threat is detected, AgileBlue Cerulean automatically triggers a playbook of response actions. Our platform integrates with your existing security tools, so you can take action directly from the AgileBlue dashboard.

Support
When and if you need additional support, our team of security experts is always available to assist 24/7. We're committed to providing you with the security you need to protect your business.

Protect your organization with unparalleled efficiency, speed, and precision. Stay one step ahead of cybercriminals with our cutting-edge threat detection capabilities. AgileBlue Cerulean analyzes vast volumes of data in real time, effortlessly identifying patterns, anomalies, and indicators of attack. Our platform learns from each attack, continuously adapting and improving its defense mechanisms. Stay ahead of emerging threats, leveraging the power of automated intelligence to safeguard your critical assets and sensitive information. AgileBlue Cerulean also seamlessly integrates with your existing security infrastructure, augmenting your current tools and workflows.

AGILEBLUE

WE'VE GOT YOU COVERED.

AgileBlue is proven to detect cyber threats faster and more accurately across your entire digital infrastructure and cloud. We provide 24/7 monitoring, detection and response to identify cyber threats before a breach occurs.

AgileBlue Cerulean is an AI-based SOC|SOAR platform that uses the power of AI to make cybersecurity more responsive and adaptive. Our AI technology accelerates detection and increases the speed of response, while at the same time providing human touch. Our AI-driven platform provides the perfect combination of automation and people, allowing us to mitigate your cyber risk by moving quickly and confidently.

For more information, visit our website: AgileBlue.com

Ready to start protecting your company?

REQUEST A DEMO