From Threats to Defense:

Harnessing AI in the Battle Against Cyber Attacks

Whitepaper

2023

AGILEBLUE

INTRODUCTION TO AI

Artificial Intelligence (AI) enables machines to imitate human intelligence, facilitating learning, reasoning, and autonomous decision-making, with profound implications for various industries. Its ability to enhance efficiency, accuracy, and decision-making processes has greatly impacted today's society. It also automates and optimizes processes which provides valuable insights and predictions, fosters innovation, and largely improves overall quality of life. AI drives breakthroughs in technology-driven fields like autonomous vehicles, natural language processing, and robotics. It enables the creation of innovative products and services that enhance convenience, productivity, and efficiency, shaping a future where intelligent machines collaborate with humans to tackle complex challenges and drive progress.

AI-driven cybersecurity tools can bring savings of

$2.9 million

on average for a U.S. company.

Source: Gitnux

Understanding the Threat Landscape

In the digital age, cybersecurity is crucial due to society's reliance on technology. The widespread use of interconnected devices poses heightened cyber-attack and data breach risks, necessitating protection of sensitive information, critical infrastructure, and privacy. Traditional cybersecurity measures have limitations in combating evolving threats, but the introduction of artificial intelligence (AI) offers promising solutions. AI, with advanced algorithms and machine learning techniques, enables faster threat detection, proactive threat hunting, and automated response, enhancing security and mitigating risks in the digital landscape.

AI-POWERED CYBER-THREATS

- **Deepfake Attacks**
- **AI-Powered Malware**
- **Advanced Persistent Threats (APTs)**
- **AI-Powered Phishing Scams**
- **DDoS Attacks**

Enhancing Cybersecurity With AI

Machine Learning Algorithms for Anomaly Detection

Machine learning (ML) is a subset of artificial intelligence that enables computer systems to learn and improve from data without being explicitly programmed through the use of algorithms and statistical models to analyze and draw inferences from patterns in data. Machine learning can provide the following in cybersecurity:

- Improved malware detection from the ability to identify and remember characteristics and behaviors of known malware
- Assist in vulnerability management by identifying potential weaknesses in systems
- Automate incident response processes, allowing for rapid and efficient threat mitigation.
- Monitor network traffic for anomalous behavior, aiding in the detection of network-based attacks and data exfiltration attempts.

Artificial Intelligence in SOAR

By harnessing artificial intelligence (AI) and machine learning, SOAR automation can effectively analyze and adapt insights provided by analysts, enabling the prioritization of threats, making recommendations, and automating future response actions.

Top 3 Uses:

1. **Threat Prioritization:** AI in SOAR cybersecurity prioritizes threats by analyzing data based on severity and potential impact, allowing security teams to focus on critical incidents and optimize response efforts.

2. **Automated Response Actions:** AI-powered SOAR platforms swiftly automate response actions, leveraging machine learning algorithms, predefined playbooks, and contextual information to isolate affected systems, block malicious IP addresses, and initiate incident investigations, effectively reducing response time and minimizing security incident impact.

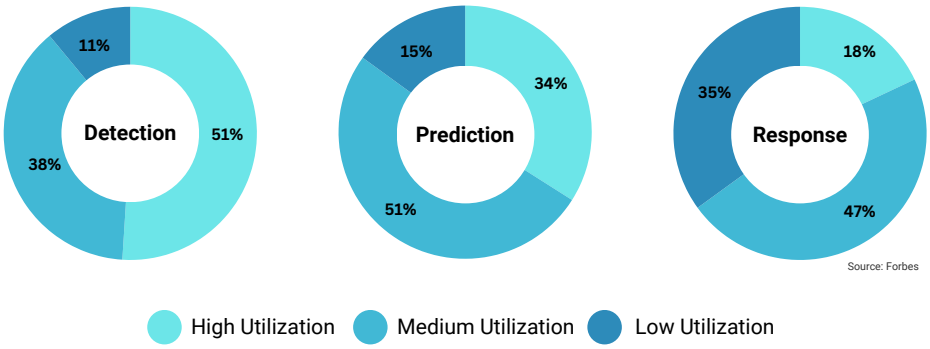
3. **Intelligent Recommendations:** AI-driven SOAR systems analyze historical data, security trends, and contextual information to intelligently recommend effective response actions, offer insights on incident handling based on past incidents, and identify overlooked patterns and correlations, enhancing decision-making capabilities for improved outcomes.

AI-Powered Threat Detection and Prevention

Threat Detection: Approximately 90% of threats can be detected using traditional techniques, but by implementing AI, the detection rates can be raised to approximately 95%. However, this shift may lead to a higher occurrence of false positives. The optimal approach involves a combination of both traditional methods and AI, which can achieve a much higher detection rate while minimizing false positives.

Threat Prevention: The implementation of advanced AI technology significantly expedites the process of detecting cyber threats, resulting in an acceleration of approximately 73% compared to traditional detection methods.

A Typical Organizations Utilization of AI in Cybersecurity



AI in Behavioral Analytics for UEBA

- User and entity behavior analytics (UEBA) can leverage artificial intelligence to detect anomalous user behavior patterns that may indicate a potential security breach. For example, an AI-powered UEBA system can analyze login data, network activity, and application usage to identify deviations from normal behavior.

- By integrating machine learning algorithms, UEBA can dynamically adapt to evolving cybersecurity threats and recognize new attack patterns. For instance, an AI-driven UEBA solution can continuously analyze large volumes of data from various sources, such as endpoints and cloud platforms, to identify emerging attack vectors and provide real-time alerts.

- Artificial intelligence can enhance UEBA's ability to accurately distinguish between genuine user activities and malicious actions, reducing false positives. For instance, an AI-enabled UEBA platform can utilize natural language processing (NLP) algorithms to analyze employee communication patterns, helping to differentiate between regular conversations and potentially malicious conversations involving data exfiltration or unauthorized access attempts.

FUTURE TRENDS & CHALLENGES

In the future, AI and ML are expected to play an increasingly vital role in cybersecurity. Here are some examples of how these technologies could be leveraged in the future to enhance the security of organizations:

- **AI-Driven Incident Response and Forensics:** Data from multiple sources including network traffic, endpoint data, and logs can be automatically analyzed, allowing for real-time threat identification and response. This capability enables organizations to promptly contain and investigate incidents quickly.

- **The Intersection of AI and Blockchain:** The integration of AI and blockchain technology offers a resilient and decentralized approach to cybersecurity, particularly in the realms of identity and access management, secure data sharing, and robust payment systems.

- **AI-Driven Security Operations Centers (SOC):** AI and ML have the potential to enhance the efficiency and efficacy of security operations centers (SOCs) through automating repetitive tasks, analyzing data from diverse sources, and delivering real-time threat intelligence.

As AI continues to evolve, it is poised to revolutionize the field of cybersecurity, empowering security professionals with advanced tools and capabilities to stay ahead of increasingly sophisticated cyber threats.

However, AI in cybersecurity also presents several challenges that need to be addressed for its effective implementation. These challenges include:

The global artificial intelligence in cybersecurity **market size** is expected to hit around **$102.78 billion by 2032**, growing at a **CAGR of 19.43%** between 2023 and 2032.

Source: Precedence Research

Bias in AI Systems: The potential for bias in AI systems can result in compromised threat detection accuracy and false positives, consequently squandering resources and generating a misleading perception of security.

Regulatory Compliance: The regulatory landscape concerning the utilization of AI in cybersecurity is continuously evolving, necessitating organizations to ensure that their AI deployments align with applicable laws and regulations.

Adversarial Machine Learning: The utilization of machine learning algorithms by cybercriminals can enable them to circumvent AI-powered security measures, posing challenges for organizations in effectively defending against cyber-attacks.

Automate your Cybersecurity With 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