ACRISURE®

LONDON WHOLESALE

Cyber Threat Intelligence Report

in partnership with Cybeta

ACRISURE® LONDON WHOLESALE

ACRISURE®

ABSTRACT: Artificial Intelligence (AI) has emerged as a transformative technology in various sectors, including cybersecurity. Yet, little if anything about the advancement's true effect is predictable. How much is AI already a part of cyber defenses, where can it improve and how might attackers also benefit from such advancements? Today we explore the possible and profound impacts of AI on cybersecurity, how it can enhance threat detection, streamline incident response, and introduce new challenges in the ongoing battle against cyber threats. We will highlight the potential benefits and risks associated with the integration of AI into cybersecurity tactics for both attackers and defenders.

Introduction

Cyber threats continue to increase in sophistication, posing significant challenges to the security of data and systems. So the question now becomes whether AI can emerge as a powerful ally for cybersecurity professionals or are potential benefits offset by the value to attackers.

AI, encompassing machine learning, deep learning, and natural language processing, offers advanced capabilities for analyzing vast datasets and identifying anomalies, thereby strengthening cyber defense mechanisms. The positive impacts of such capabilities are AI's role in threat detection, incident response, and preemptive attack intelligence.

AI-Powered Threat Detection

Although recent articles tend to discuss AI as a "new capability", the reality in cyber is that various iterations over the last decade of AI have already revolutionized how organizations detect cyber threats. Traditional signature-based detection systems are limited in their ability to identify new or evolving threats because, by definition, they require the presence, detection, logging and then inclusion of a threat after it has already appeared in the wild. Conversely, AI-driven threat prevention can utilize machine learning algorithms that adapt and learn from historical data.

a. Anomaly Detection: AI can identify anomalies in network traffic and user behavior. Machine learning models establish a baseline of normal behavior and quickly detect deviations, which are often indicative of malicious activity. By continuously learning from new data, AI-driven systems can adapt to emerging threats and reduce false positives. The more AI can observe regular network traffic and user behavior, the better and more efficient the same Anomaly Detection system should perform in identifying deviations.

b. Predictive Analysis: Through data analysis, machine learning algorithms can identify trends and behaviors that might lead to security incidents. This proactive approach allows organizations to take preventive measures before threats escalate.

c. Phishing Detection: Phishing attacks historically and continuously persist as the threat vector of choice for most cyber intrusions. AI-powered email filtering systems employ natural language processing to analyze email content, sender behavior, and contextual information to detect phishing attempts.

AI-Enhanced Incident Response

In addition to predictive threat detection, AI will play a pivotal role in next generation incident response.

a. Incident Triage: AI-driven incident response platforms can quickly prioritize and categorize security incidents based on their likely severity, which allows security teams to allocate their resources efficiently.

b. Threat Hunting: By sifting through massive datasets, AI algorithms uncover hidden threats that might evade traditional security measures by identifying unusual patterns.

c. Real-time Threat Analysis: AI systems can more rapidly analyze large data from various sources and provide insights that focus security teams and enable quick decisions and timely responses.

Challenges and Ethical Considerations

While AI may eventually revolutionize cybersecurity, like most technological advancements, it also presents significant challenges and even ethical considerations.

a. False Positives and Negatives: Information overload and alert fatigue are significant challenges and resource drains in cyber security. AI-powered systems are not immune to errors and, if improperly configured or used, can result in outputs of limited value. False positives lead to unnecessary alerts and resource drain, while false negatives can allow threats to go undetected. Continual refinement of AI models is essential to mitigate these issues.

b. Adversarial Attacks: Cybercriminals are actively seeking ways to exploit AI systems, using novel attack techniques to trick machine learning models into making incorrect predictions and thereby escaping detection. This ongoing back-and-forth demands constant vigilance and adaptive AI defenses. In addition, the same logic that allows AI to identify threats can and is easily adapted by attackers to identify weaknesses and execute efficient attacks. Limitations on the types of questions that can be asked and answered by AI are not perfect blocks against the collection of offensive cyber vulnerability information that is extremely helpful to a would-be attacker.

c. Skilled Workforce: There is a global shortage of cyber security professionals within the commercial sector. The integration of AI into cybersecurity necessitates a more skilled workforce capable of developing, implementing, and maintaining AI systems. In the near term, this is likely to exacerbate the existing resource shortage while potentially offering a glimmer of hope by automating more elements of cyber security.

Conclusion

Artificial Intelligence's ability to analyze vast amounts of data, detect anomalies, and enhance incident response capabilities has made it an indispensable tool in the ongoing battle against cyber threats. However, as with any technology, AI in cybersecurity comes with challenges and ethical considerations that must be carefully managed. Most critically, we have yet to fully grasp the potential increase in efficiency and lethality of cyber attackers who leverage the same strengths of AI in pursuit of their own objectives.

Organizations must invest in both AI technology and the development of human expertise to harness the full potential of AI in cybersecurity. AI is not a panacea for all cybersecurity challenges, but can be a powerful ally that, when properly implemented and managed, can significantly enhance an organization's efficiency and ability to protect its data and systems. Conversely, it can potentially arm hackers with increasingly effective attack tactics. This dichotomy will end up determining if AI is a net benefit to cyber security or yet another example of the cat and mouse attackers and defenders will always experience. In fact, it was an AI natural language model that identified and authored much of this paper, showing that even AI itself cannot fully decide whether its overall impact to cyber security will be positive or negative.

About Acrisure London Wholesale and Acrisure Re

The Acrisure London Wholesale team are uniquely placed within the market to offer excellent solutions to our clients, with both scale and breadth. We focus on both one-off open market/brokerage placements as well as designing and sourcing capacity for programs. Our analytics team allows us to provide outstanding results for our many independent retail and wholesale broker partners.

Acrisure Re is a full-service (re)insurance intermediary and capital management advisor with a commitment to providing tailored risk transfer solutions for our clients. With our global team of more than 350 experienced and talented employees dedicated to providing bespoke advisory, portfolio, and reinsurance solutions, we are driving a sophisticated, tech-enabled future for the (re)insurance industry.

About Cybeta

Cybeta was founded by a specialized group of senior Intelligence Community officers with 75+ years of combined experience in the United States Central Intelligence Agency, National Security Agency, and Department of Defense. The team worked together as information operations officers targeting and extracting priority objectives from the most advanced cyber adversaries. Their skills, combined with advanced data analytics and machine learning expertise, has led to Cybeta's unparalleled productized cyber services.

Contact:

Tom Quy
Senior Vice President
tquy@AcrisureWS.com

Luke Lattner
Vice President
Luke.Lattner@cybeta.com