

AI-Powered Defense: Protecting Data in the Digital Age

*1Pamela Nvatsine

^{*1}Masters in Technology Cloud Computing, Department of Information Technology, Fortinet NSE3, EC Council Ethical Hacking, Kaspersky NEXT, Zimbabwe.

Abstract

Artificial intelligence has the immense capability to detect zero day attacks like no other solution or human could. However, both bad actors and providers of cybersecurity solutions are employing the artificial intelligence. Human intervention is still a necessity in mitigating attacks however. The algorithm that employs generative AI is able to learn its environment and to provide solution to while constantly adapting to the changing landscape. AI has the capacity to keep pace with cybersecurity, which is a moving target. Machine speed is required to stay ahead of the threats. Social engineering remains a key factor in hacking; AI can be trained to detect social engineering threats with accuracy and programmed with relevant action to take in the event that a social engineering threat is detected.

Keywords: Artificial Intelligence, cybersecurity, recovery, threat detection and response, vulnerabilities, cyber drills

Introduction

Cybersecurity's importance has peaked and will remain high as organizations and individuals adopt cloud and digital technologies for business and personal use. Cyber threats are inherent with the use of cloud technologies. The threats can be external or internal in the case of organizations. Bad actors adopt various methodologies in order to exploit vulnerabilities in a network. There is a general skills shortage in the cybersecurity space with many organizations offering free awareness and skills training to ease the burden.

Many providers of cybersecurity solutions are employing artificial intelligence to mitigate these attacks and to find vulnerabilities before a hacker or other bad actor does. One such organization is Dark Trace that offers artificial intelligence based cybersecurity in a discourse paper they emphasize the need for cyber resilience. AI's computational power needs to be balanced with human intuition and contextual thinking to achieve information security overall. A self-learning AI model empowers the organizations cybersecurity front by providing protection that is specific to the needs of the institution as each organization is unique. Review Method Selection Criteria for papers





Some Ways AI Is Employed in Cybersecurity

Artificial intelligence will assist the banking and finance industry to mitigate cyber threats. https://ejeng.org/index.php/ejeng/article/view/3103. Log data can be analyzed in order to detect anomalies. An approach of converting diverse log data into graphs and detecting anomalies using deep learning methods will prove effective in

mitigating threats. Human and AI collaboration can be employed to provide comprehensive information security in a rapidly shifting digital age.

Cyber-attacks that utilize AI are on the rise, in light of this cybersecurity needs to employ artificial intelligence to match the threats and perhaps predict future attacks. AI is better able to adapt to threats and identify vulnerabilities than human

*Corresponding Author: Pamela Nyatsine

beings, as the speed at which threats are being churned out is extremely high. AI can fill the skills gap mentioned earlier through processing power and utilizing algorithms that can study behavior of network users in order to detect anomalies. There are a number of advantages to using AI such as its ability to compare past attacks with current attacks in order to predict future attacks. Privileged access can be monitored and any changes can be studied as they can be a potential threat.

Through social engineering bad actors seek to gain access to networks in order to compromise the system or swindle the users of resources after stealing credentials. AI studies behavior of users on a system to do two main activities one is to know the users general behavior so that in the event an actor gains access pretending to be an authorized user but behaving differently, the AI powered cybersecurity can quickly report on this anomaly. The second way AI can assist is by studying the behavior of users to determine who is inclined to fall for social engineering traps in a given network. This is a more preventative measure that can save the organization resources.

Harnessing the processing capabilities of AI can enhance the compliance of systems with general data and network compliance standards. Every organization has to adhere to various compliance standards and there can be overlap in ensuring that this is completed at regular intervals. AI assists by providing timeous notifications on any anomalies that have been programmed into it and it can learn using algorithms to maintain this compliance standard.

There's a change in the attack surface ITU conducts cyber drills to test system vulnerabilities in organisations. The cyberdrills show an organisations readiness and assesses the strength of policies, processes to prevent or recover from cyber-attacks.



Fig 2: Exposure Management Tenable

Corporate cybersecurity management intersects with knowledge management, therefore it's crucial to employ AI to mitigate threats.

AI in SOC and SIEM

SOC Security Operations Center and SIEM Security Incident Event Management can be augmented by the incorporation of artificial intelligence. Traditionally SOC works with known signatures to mitigate attacks however it is rare that attackers use these known signatures. AI can then be used to detect these little known signatures before they attack.

Prompt engineering uses AI to attack systems therefore AI inbuilt in the defense of the system becomes a necessity. Prompt engineering is designing and refining prompts to receive responses from artificial intelligence models. According to Pasamonik *et al*, AICyberSec chatbot introduces an innovative approach to cybersecurity awareness. Cybersecurity awareness is impacting users of digital technologies an AI CyberSec chatbot.

Conclusion

Artificial intelligence in cybersecurity is the best approach to detect and respond to cyber threats in real-time. Artificial intelligence can be paired with human intuition for contextual relevance and to avoid ethical compromises. Compliance and laws may need to be adjusted to better handle the AI which is rapidly evolving.

References

- Abbas R, Michael K, Pitt J, Vogel KM, Zafeirakopoulos M. Artificial Intelligence (AI) in Cybersecurity: A Socio-Technical Research Roadmap. *The Alan Turing Institute*, 2023, 2-44.
- 2. Alaca Y, Celik Y, Goel S. Anomaly Detection in Cyber Security with Graph-Based LSTM in Log Analysis. *Chaos Theory and Applications in Applied Sciences and Engineering*, 2023, 188-197.
- 3. Allen JC. Innovating Cyber Recovery-Key to Cyber Resilience, The Dynamic Real-Time Approach to Recovering. 7, 2022.
- 4. Dark Trace Holdings Limited. Dark Trace Products & Services, 2022.
- Herman YJ, Frederic O. Study on the use of Artificial Intelligence for Cybersecurity in Companies: Case of Companies in Burkina Faso. *Scientific Research*, 2023, 15(12).
- 6. International Telecommunication Union. (2021). Operational Framework and Guidelines for the Planning and Execution of ITU Regional Cyberdrills. Geneva, Switzerland.
- 7. Jonas D, Yusuf NA, Zahra AR. Enhancing Security Frameworks with Artificial Intelligence in Cybersecurity. *International Transactions on Education Technology* (*ITEE*), 2023, 83-91.
- 8. Lalithambikai S, Usha G. Cybersecurity Unveiled: Navigating Evolving Threats And Innovations. *Fusion of*

Knowledge Multidisciplinary Perspectives in Research. Lunawada: Paradox International Publications Guide House, 2023, 118-218.

- Pasamonik D, Smolarski B, Strynkowska W, Lubicka P, Eksman M, Perli 'nski P,. Wo 'zna-Szcze'sniak, B. AICyberSec: A Cyber Security Tool. *Preprints.org*, 2023, 1-11.
- Sarker IH, Janicke H, Mohammad N, Watters P, Nepal S. AI Potentiality and Awareness: A Position Paper from the Perspective of Human-AI Teaming in Cybersecurity, 2023, 2-10.
- 11. Tahir F, Khan M. A Narrative Overview of Artificial Intelligence Techniques in Cyber Security. *EasyChair Preprint*, No 11447, 2023.
- 12. Vance TR. Artificial Intelligence in Cybersecurity: A Survey of National Research, Investment and Policy Implementation. International Journal of Computer Science and Information Technology Research, 2023, 18-25.
- 13. Veselinovic N, Milasinovic M, Jovanovic M, Aleksic A, Biga N. Countering Cybersecurity Threats with AI. International Conference on Business Information Security. Belgrade, 2022, 1-7.