



International Journal of Research in Academic World



Received: 02/July/2024

IJRAW: 2024; 3(8):129-131

Accepted: 07/August/2024

AI-Powered Defense: Protecting Data in the Digital Age

*¹Pamela Nyatsine

*¹Masters 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

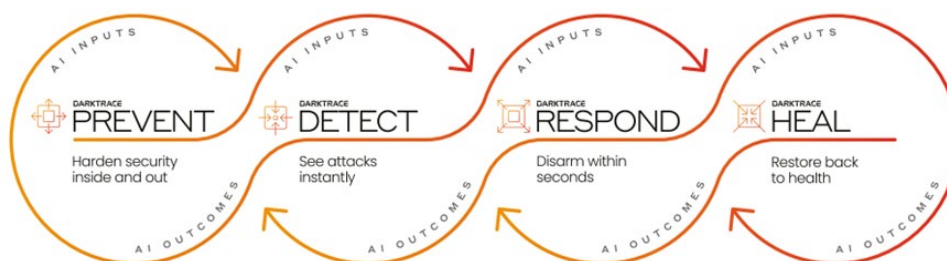


Fig 1: Cyber AI Loop

Some Ways AI Is Employed in Cybersecurity

Artificial intelligence will assist the banking and finance industry to mitigate cyber threats. <https://ej-eng.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

- Knowledge Multidisciplinary Perspectives in Research*. Lunawada: Paradox International Publications Guide House, 2023, 118-218.
9. Pasamonik D, Smolarski B, Strynkowska W, Lubicka P, Eksman M, Perliński P., Woźna-Szcześniak, B. AICyberSec: A Cyber Security Tool. *Preprints.org*, 2023, 1-11.
 10. 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.