The Debate

The benefits of Generative AI and its Impact on Network Security

By Team 3

- Shashank Phatak
- Alanood Alkuwari
- John Heart Ojabo

University of Essex Online

Introduction

Enhancing Network Security with AI:

- Automates repetitive tasks, improves threat detection, and reduces human error for safer and more efficient networks.

Adaptability to Evolving Threats:

- AI adapts in real-time to emerging cyber threats, ensuring continuous network protection.

Tool Case Study 1 - QRadar

What is QRadar

- An IBM tool that enhances network security by analysing data and detecting threats.

Advanced Features

- Detects patterns in large data sets and automates sorting security alerts.

Key Benefits

- Saves time for security teams and allows focus on critical challenges.
- Provides clear, actionable reports for better decision-making.

AI Integration

- Combines with AI to ensure faster, safer, and more efficient cybersecurity operations.

Tool Case Study 2 and 3- SentinelOne and Darktrace

- By leveraging advanced algorithms, AI-powered solutions (like SentinelOne and Darktrace) can analyse vast amounts of data in real time, identifying anomalies and potential threats that might otherwise go unnoticed (Rayhan, 2024; Orion Networks, 2024).
- It is known that up to 71% of the tasks carried out by security teams can be automated (by AI). This enables security teams to focus on other things and to respond to incidents more effectively (Accenture, 2024)
- AI tools exist already that help in this human-AI collaboration:
  - **SentinelOne:** is a leading endpoint protection platform that uses AI to monitor endpoints for suspicious activities and respond before they affect the system or even attempt to spread (SentinelOne, 2024).
  - **Darktrace:** has a self-learning AI technology that can autonomously detect and respond to cyber threats that go beyond the means of traditional security solutions (Darktrace, 2024).

Tool Case Study 4 – Abnormal Security

- Founded in 2018, Abnormal Security provides a cloud-native email security platform that uses AI-driven **behavioural data science to prevent socially engineered** and unseen email attacks that bypass traditional secure email gateways (SEGs).

- Abnormal tool protects against various threats, including business email compromise, phishing, malware, ransomware, social engineering, spam, supply chain attacks, and internal account compromise.

- The tool offers inbound email security, account takeover protection, and SOC automation. The API-based approach can enhance SEGs or function independently to bolster cloud email security and integrate with Microsoft 365 or Google Workspace.

Conclusion

- While challenges might exist, advancements in AI technology and cybersecurity practices address many of these concerns. A thoughtful, well-implemented approach to generative AI can maximise its benefits while minimising potential drawbacks.

- We believe that generative AI can revolutionise network security operations. Automating routine tasks such as threat detection and response enables organisations to streamline workflows and enhance efficiency. This, in turn, allows human resources to dedicate their expertise to addressing more complex security challenges and engaging in strategic planning, thereby fostering a more robust and proactive security posture.

References

1. Rayhan, A. (2024) *Cybersecurity in the Digital Age: Assessing Threats and Strengthening Defenses*. Available from: https://www.researchgate.net/profile/Abu-Rayhan-11/publication/380205137_Cybersecurity_in_the_Digital_Age_Assessing_Threats_and_Strengthening_Defenses/links/663104807091b94e93e7cdda/Cybersecurity-in-the-Digital-Age-Assessing-Threats-and-Strengthening-Defenses.pdf [Accessed: 26 November 2024].

2. Orion Networks (2024) *The Impact of Generative AI on Cyber Security* Available from: https://www.orionnetworks.net/the-impact-of-generative-ai-on-cyber-security [Accessed: 26 November 2024].
3. Accenture (2024) *How is AI shaping the cybersecurity strategies of tomorrow?* Available from: https://www.accenture.com/us-en/blogs/security/how-ai-shaping-cybersecurity-strategies [Accessed: 26 November 2024].

4. SentinelOne (2024) *The AI SIEM for the Autonomous SOC* Available from: https://www.sentinelone.com/platform/ai-siem/ [Accessed: 26 November 2024].
5. Darktrace (2024) *Darktrace Autonomous Response Keeping pace with evolving threats* Available from: https://darktrace.com/darktrace-autonomous-response [Accessed: 26 November 2024].
6. IBM Corporation (2023) QRadar SIEM: Security Intelligence and Analytics. Available from: https://www.ibm.com/products/qradar-siem [Accessed 26 November 2024].
7. Nguyen, D.M. & Lin, C.W. (2023) Generative AI in Cybersecurity: Enhancing Threat Detection and Adaptation. Journal of Cybersecurity Trends, 12(3), pp. 45-58.
8. Smith, A. & Patel, R. (2023) AI-Driven Approaches to Network Security: Real-Time Adaptability and Efficiency. Cybersecurity Advances, 18(2), pp. 89-102.
9. Smith, J. & Brown, T. (2022) Enhancing Network Security with IBM QRadar: Tools and Techniques. Journal of Cybersecurity Innovation, 10(4), pp. 123-135.
10. How Abnormal Security protects workforces from email attacks | Cyber Magazine
11. Customer review: Abnormal Security helps protect our environment with next-gen email security | Microsoft Community Hub


Thank you!