Collaborative Discussion 1: The 4th Industrial Revolution Summary Post

In the ever-evolving landscape of cybersecurity, the intersection of artificial intelligence (AI) and data science emerges as a pivotal force, transforming how organisations approach threat detection and mitigation. The discussion around the TalkTalk and Equifax breaches underscores the critical need for robust cybersecurity measures. The repercussions of these incidents extend beyond financial losses, impacting customer trust and organisational reputation. The growing threat landscape, marked by the release of 500 million new types of malware in 2015, emphasises the importance of staying ahead of adversaries. Machine learning, with its predictive capabilities, proves instrumental in bolstering cybersecurity. Fraley and Cannady's (2017) research showcases the potential of classification models to predict security events with high accuracy, reducing analysis time significantly.

The role of AI in geographical analysis and capability development adds another layer to this narrative. While AI and machine learning present opportunities for efficiency gains, caution is urged against viewing these technologies as direct replacements for skilled professionals. Instead, they should be harnessed as supplementary tools, enabling analysts to focus on higher-order tasks that demand creativity and critical thinking. This approach aligns with the exponential growth and trendiness of data science roles (Englmeier and Murtagh, 2017), positioning data scientists and analysts to lead innovation in their respective fields. Schwab & Zahidi (2020) states that when compared to previous years job creation is slowing while job destruction accelerates.

The transformative impact of AI is further evident in the realm of mobile security, where traditional protection measures often fall short against Advanced Persistent Threats (APTs). The proactive nature of AI in threat detection on mobile devices showcases its potential to provide a robust defence against evolving security challenges (Al-Kadhimi, 2023). As we navigate this dynamic landscape, the collaborative integration of human expertise and technological prowess emerges as a key strategy, ensuring not only enhanced security but also innovation and resilience in the face of cyber threats.

References:

Al-Kadhimi, A. et al. (2023) A Systematic Literature Review and a Conceptual Framework Proposition for Advanced Persistent Threats (APT) Detection for Mobile Devices Using Artificial Intelligence Techniques. Applied Sciences, 13(14): 8056. DOI: https://doi.org/10.3390/app13148056

Englmeier, K. and Murtagh, F., 2017. Editorial: What Can We Expect from Data Scientists. Journal of theoretical and applied electronic commerce research, [online] 12(1), p.i-v. Available at:

<https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-18762017000100001&lng=en&nrm=iso&tlng=en> [Accessed 23 September 2022].

Fraley, J.B. and Cannady, J. (2017) ‘The promise of machine learning in Cybersecurity’, *SoutheastCon 2017* [Preprint]. doi:10.1109/secon.2017.7925283.

Janakiraman, R., Lim, J.H. and Rishika, R. (2018) ‘The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer’, *Journal of Marketing*, 82(2), pp. 85–105. doi:10.1509/jm.16.0124.

Schwab , K. and Zahidi , S. (2020) *The Future of Jobs Report 2020*, *World Economic Forum*. Available at: https://www.weforum.org/publications/the-future-of-jobs-report-2020/ (Accessed: 22 November 2023).