Your post is an insightful introduction to Artificial Intelligence (AI) and Intrusion Detection Systems (IDS) with regards to their use in cyber security.

I agree with your views on the downsides to AI when utilised to combat cyber security threats. Up until recently, there has been no legislation to govern the use and development of AI. It wasn’t until March 2024 that the European Parliament voted to adopt a landmark law governing its use (European Parliament, 2023). In my opinion, such a lack of regulation leads to the possibility of tainted training data, diminishing AI’s usefulness.

On another note, AI based IDS have been shown to improve accuracy in combatting cyber attacks, however do come with their downsides (Sowmya, 2023). An exploration into this topic would certainly enhance your post.

In conclusion, this is a well presented introduction to AI and IDS. To improve your post, it would be interesting to hear your views on integrating the two technologies.

References

European Parliament (2023) EU AI Act: first regulation on artificial intelligence. Available from : <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> [Accessed 17 June 2024].

Sowmya, T. & Anita, M. (2023) A comprehensive review of AI based intrusion detection systems. *Measurement: Sensors* 28(100827). DOI: <https://doi.org/10.1016/j.measen.2023.100827>

This is a well researched post on Multi-Factor Authentication and Cloud Based Intrusion Detection Systems. The introduction to computer systems architecture and software and network security effectively set the scene for the remainder of the post.

As Sinigaglia (2020) states, “When properly designed and implemented, MFA protocols provide strong security guarantees.” I agree that social engineering is an issue. However, when taking into account the implementation of MFA and the quote from Sinigaglia, I would argue that social engineering isn’t necessarily issue with MFA. It is more an issue with authentication and password protection in general.

What would be your opinions on the above argument? Also, how much stronger are MFA mechanisms compared to single factor authentication mechanisms?

To sum up, this is a well formatted post on MFA and CIDS. Further discussion on the benefits of such technologies will help strengthen the post.

References

Sinigaglia, F. et al. (2020) A survey for multi-factor authentication for banking in the wild. *Computers & Security* 95(101745). DOI: <https://doi.org/10.1016/j.cose.2020.101745>

I enjoyed reading your post on malware and the technologies used to combat such a threat. The post has a strong structure and all explanations are well articulated.

While effective at detecting exploits in the early 2000s, antivirus software is noticeably less efficient in todays era. This is due to attackers “living off the land” and evading the threat detection measures utilised by AV products (Anderson, 2020). You rightfully pointed this out, which leads onto the topic of Endpoint Detection and Response.

An exploration into the workings of Endpoint Detection and Response would be beneficial in order to enhance your post. EDR collects data from all endpoints in a network and provides tools for a security team to discover and prevent emerging threats by themselves (IBM, N.D.). In my opinion, this is an extremely impactful area of cyber security that is worthy of further discussion.

In conclusion, this is a strong introduction to malware and the technologies used to prevent this threat. It will be interesting to read more about your views on EDR.

References

Anderson, R. (2020) *Security engineering: A guide to building dependable distributed systems.* Indianapolis, Indiana: John Wiley & Sons, Inc. DOI: 10.1002/9781119644682

IBM (N.D.) What is endpoint detection and response (EDR)? Available from : <https://www.ibm.com/topics/edr#:~:text=What%20is%20EDR%3F,other%20traditional%20endpoint%20security%20tools>. [Accessed 17 June 2024].