Ethical Reflection - Johny Son 22169335

Ethical Reflection:

Some ethical concerns regarding AI usage within open-source software security includes privacy issues. This is due to some security solutions requiring data collection in order to tackle certain threats. Anomaly detection is a good example for a solution that requires data detection. The system normally need data of normal activities to compare with new data to detect any outliers and anomalies which often indicate signs of hacking, bank fraud, malfunctioning equipment, structural defects / infrastructure failures, or textual errors (AVI Networks, n.d.). In addition, another ethical issue is security risk. There are adversarial attacks where the attacker manipulates the AI into sending out false positives and incorrect feedback. Attackers use this method in hopes of financial and data gain, which connects to this point to the previous one about privacy concerns (dremio, n.d.).

Personal Reflection:

Although there are downsides, the reason we chose this as our topic is because of it's upsides, which includes collaboration (Ahmad, 2023). I believe that collaboration alone is the greatest benefit of them all. In open-source communities, it is common to follow ethical guidelines when developing AI security tools. Additionally, education is another benefit from AI security OSS, as open-source projects often have useful educational resources for aspiring developers and students which helps promotes deeper understandings of AI security.

Recommendations:

There are many downsides and upsides, however, I believe that AI cybersecurity is the future of all tech based security. The advancement of AI is both good and bad in different ways. Some recommendations I would give to avoid the downsides are, promoting diverse collaboration, adversarial trainings and following guidelines. I believe the first step to solving cyber threats is to avoid it. It is easier to prevent than to fix, therefore minimising all the possible threats in your security should be prioritised. This could easily be done by following and promoting coding practices. Promoting diverse collaborations is great because a wide range of perspectives and opinions can help spot mistakes in codes more efficiently than just a single point of view. Like mentioned

previously, adversarial training is good at preventing threats by improving the codes ability to detect and recognise adversarial attacks.

In summary, there may be many problems and issues with AI security, but as technology advances, there will be more solutions towards the current issues. I believe that there is currently a good balance between threats and issues, and open-source AI security is a good option for those who need cheap good security for their software. The issue is whether or not high-risk organisations such as financial institutions and healthcare providers should convert to using AI security given its current state. However, AI has the ability to self-learn therefore helping it advance faster than other modern day security solutions.

References

Ahmad, R. (2021). A critical review of open source software development: Freedom or benefit libertarian view versus corporate view. *IT Professional, 23*(1), 16-26. https://doi.org/10.1109/mitp.2020.3014450

AVI Networks. (n.d.). Anomaly Detection. https://avinetworks.com/glossary/anomaly-detection/

dremio. (n.d.). Adversarial Attacks in AI. https://www.dremio.com/wiki/adversarial-attacks-in-ai/