Some great points made in this discussion by all. The amount of time and cost that goes into detecting a breach and resolving it is vast. There are some great observations on AI and ML being used for cyber security.

After reading this discussion, I was curious to know how many new vulnerabilities were introduced in any given year. I found an IEEE Computer Society publication, which indicated that there were over twenty thousand new vulnerabilities in 2019 and this had increased over 17% over the previous year. Having a team manually trying to detect and investigate each of these will take up so much time and effort.

There is also the argument as to how you prioritise which vulnerability should be investigated first or which vulnerability would have more impact to an organisation, for example the log4j vulnerability (CVE-2022-23307) which was found late last year and Microsoft Excel Remote Code Execution Vulnerability (CVE-2022-21841). Having dedicated teams who know the environment inside out would be beneficial but the sheer volume of vulnerabilities is overwhelming. Organisations definitely need to consider employing sophisticated tools to help identify a true threat.

Segal, E (N.D.). The Impact of AI on Cybersecurity

https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity [Accessed 15 March 2022]