Read Chapter 16: Next Generation Security Threats: Why Cyber was Only the Beginning in the Future Crimes book. Prepare responses to the following question.

Research how IBM's Watson is being used in cybersecurity.

Named after IBM's founder, Thomas J. Watson, IBM's Watson is a supercomputer that uses Artificial intelligence to respond to questions significantly faster than if the same questions were asked to a human being. The capability of the computer was made clear when it digested over 200 million pages of structured and unstructured data to defeat Ken Jennings, a Jeopardy contestant who won the game seventy-four times in a row.

According to chapter 16 of Future Crimes book, Watson has also been used in medicine to help doctors match patients with clinical trials. It is also used to read millions of patient's records and thousands of journal articles to assist clinicians to come up with the best treatments. However, due to IBM's huge investment, non-profits, the government, individuals, and small companies have extended the capabilities of the supercomputer. In fact, there is even a chance that the computer can be misapplied and utilized to facilitate organized crimes. Hence, hacking, identity theft, fraud, and money laundering are some of the potential crimes that can arise.

On the other hand, IBM's Watson is the first supercomputer that combines artificial intelligence and sophisticated analytical software to deter cyber threats (Goud, n.d.). It is being used in cybersecurity to help security analysts detect threats faster than ever before. That is, it allows insights from both structured and unstructured data to be combined with millions of individually logged IT events so that threats that are unnoticeable or hidden due to a manual investigation can easily be uncovered daily (Mina, 2017). Additionally, Watson is technically designed to power cognitive Security Operations centers (SOCs) and was trained on the language of cybersecurity. This enhancement provides security analysts to have a broader scope to respond to threats across endpoints, networks, users, and cloud. Furthermore, in order to extend the ability of cognitive SOC to endpoints, IBM Security also announced a new Endpoint Detection and Response (EDR) solution. The security solution helps organizations to gain a more comprehensive visibility into the evolution of the threat landscape and tighten the gap between malicious behavior detection and remediation (Goud, n.d.).

References

Mina, G. (2017). AI is the future of cybersecurity – How Watson helps detect threats faster and better protect your organization. IBM Blogs. Retrieved from https://www.ibm.com/blogs/watson/2017/08/ai-is-the-future-of-cybersecurity-how-watson-helps-detect-threats-faster-and-better-protect-your-organization/

Goud, N. (n.d.). IBM Watson Supercomputer to be used for Cyber Security. Cybersecurity Insiders. Retrieved from https://www.cybersecurity-insiders.com/ibm-watson-supercomputer-to-be-used-for-cyber-security/