The Role of AI in Strengthening Your Cybersecurity Management Systems

According to Capgemini, 69% of enterprise executives believe AI will be necessary to respond to cyberattacks, while 80% of telecom companies consider AI as the best option for cybersecurity.

AI continuously improves its knowledge to understand new threats and risks. It does this by consuming billions of data artefacts from a variety of sources such as blogs and news stories. Furthermore, it gathers insights and uses reasoning to identify the relationships between threats, such as malicious files, or suspicious IP addresses. This analysis gives your security experts the opportunity to respond to threats up to 60 times faster.

How AI Can Help by Processing and Analysing Your Data
AI can detect anomalies by first of all learning what is considered normal in your data. Any changes to data or behaviour that it regards as typical and within expected parameters will be accepted and added to your cybersecurity system's knowledge bank. Thus, when AI detects unusual trends and behaviours, it will carry out the relevant measure such as informing security analysts.

Phishing is one example where AI can protect you. Whilst research shows that 4% of all emails are phishing emails, standard security methods fail to detect nearly one third of them. AI can help you, however, by scanning the internet for phishing threats from all over the world and will advise you of them before they even reach you.

Using Algorithms for Password Protection and Authentication
AI technology can be used to generate passwords that, whilst incredibly strong, are also memorable as they are based in some way on a piece of information that is memorable to the user. This could be a song, a poem, a proverb or something else. The AI can take that information and use alternative letters, numbers, and symbols to create an unguessable password. The technology can also warn users when

passwords aren't sufficiently safe, and even advise when a password may have been compromised. Nevertheless, a password on its own is a weak defence against a ruthless and tenacious criminal, and this is where more sophisticated authentication mechanisms come in.

Multi-factor authentication, for example using a combination of password and biometric data such as the face, is already known to provide a strong defence against cyber-attack. This approach does, however, have its limitations, and attackers have been known to breach security by simply using a photograph of the user. Therefore, developers are using AI to improve the reliability of biometrics. For instance, in the case of face recognition, AI software can create a sophisticated model of the user's face by detecting essential correlations and patterns. AI then uses this information to detect anything out of the ordinary whilst allowing for differences in lighting conditions or changes such as hairstyles, hats and make-up.

Using AI to Enhance Endpoint Protection

Gathering and scrutinising endpoint data in real-time using AI methodology offers new insights into endpoint security, and is emerging as a key component of today's security information and event management (SIEM) platforms. It automatically provides continuous analysis and correlation of all activity within an IT setting.

When you introduce AI to your security operations centre (SOC), the benefits include streamlined threat detection, investigation and response processes, and increased productivity. Your analysts spend more time doing what they enjoy and you will experience a significant reduction in the cost of security breaches. AI can add value to your security personnel by helping your analysts do their jobs more effectively and efficiently.

Conclusion

Without a tough cybersecurity management system in place, your business is exposed to the danger of catastrophic damage to data, revenue, and reputation. AI can enhance your cybersecurity by automatically detecting and highlighting unusual trends and behaviours. It can improve password security and allow for more sophisticated authentication mechanisms. It can also power up your SOC and SIEM platform many times over, keeping you protected well into the future.