Fight AI with AI: The Future of Security and Risk Management

Introduction

As organisations expand their digital presence, the nature of cyber threats is rapidly changing. Attackers are now using Artificial Intelligence (AI) to develop faster, smarter and more targeted attacks. Traditional cybersecurity models can no longer keep pace with this level of sophistication.

To maintain resilience and protect critical systems, Security and Risk Management (SRM) must evolve.

The Rise of AI

Cybercriminals are using AI to scale their operations. This includes creating realistic phishing messages, scanning for vulnerabilities and launching deepfake enabled scams.

Weaponised AI

Attackers use AI to craft convincing phishing emails, often tailored using data from social media or previous breaches, increasing the likelihood of success. AI is also being used to generate malicious code, test defences and evade traditional security tools.

Automated Cybercrime

- Vulnerability scanning tools powered by machine learning can identify weaknesses in networks faster than manual methods.
- Deepfake technology is being used to impersonate staff in video or voice, enabling more effective social engineering.
- Chatbots and AI agents can simulate real-time interactions during phishing campaigns or scam calls, making them more persuasive and harder to detect.

This level of automation reduces the barriers to entry for cybercriminals and increases the speed at which attacks can be launched.

AI to strength SRM

Predictive Analytics: AI can analyse vast amounts of data to predict potential security threats before they occur. By identifying patterns and anomalies, AI helps organisations proactively mitigate risks

Automated Threat Detection: AI systems continuously monitor network traffic and user behaviour to detect anomalies and potential security breaches in real-time. This automation significantly reduces response time to threats, enhancing overall security

AI Security Management: AI TRiSM focuses on securing AI systems, ensuring transparency and building trust. This discipline addresses both technical and ethical concerns, making AI systems more reliable and secure.

The Balance

While AI offers strong benefits, it must be used responsibly. Models must be transparent and their decisions explainable. When implementing AI, organisations should keep humans involved in critical decisions, document how AI systems work and conduct regularly reviews.

Using AI without proper oversight can lead to new risks, including false positives, missed threats or biased decision making.

Conclusion

AI is changing how cyber threats are created and delivered. It is also transforming how organisations defend themselves. The most effective SRM strategies now include AI as a core component, not just a supporting tool. Attackers are using AI to get ahead. Defenders must do the same.

To protect the future, organisations must fight AI with AI.