AI may revolutionize security, but not without human intuition





Artificial intelligence (AI)-based cybersecurity isn’t a new

concept. Machine learning algorithms, deep learning techniques and other AI technologies are being used to identify malicious patterns, detect anomalies, predict threats and respond to attacks. While there is a lot of excitement and optimism around AI, a certain question arises: Can AI replace human intuition? Can it substitute for security expertise? To answer this question, security leaders must understand the advantages of AI, its challenges and its limitations.

The advantages of AI in cybersecurity

AI brings three major advantages to cybersecurity. The first is speed. There's a limit to what humans can analyze in terms of speed and scale. On the other hand, machines can analyze gargantuan amounts of data well beyond human capacity. And machines don't just analyze; they can respond to threats and report them in real time. For humans to achieve AI-like capacity, it would demand a ridiculous amount of human effort.

The second benefit AI brings to the table is accuracy. Humans are susceptible to cognitive biases. In contrast, AI is data driven – so long as it's trained on bias-free data, its decision-making will (in general) be more accurate. AI also tends to learn from new data much faster than a person can, continuously adapting its ability to detect and respond against evolving threats.

The third benefit AI delivers is automation. AI systems can autonomously correlate and analyze system and network logs, indicators of compromise (IOCs) and anomalies, detecting and responding to zero-day attacks immediately. This can be a game changer for security teams, especially at a time when cybersecurity is undergoing a talent shortage.

Limitations and challenges of AI

No doubt, AI's potential is mind-boggling. But some of its benefits are overhyped. For instance, AI speed and accuracy.

The more things machine learning flags for human review, the more time security teams spend analyzing. As a result, they might become distracted and lose sight of critical vulnerabilities. AI models can lack contextual understanding; they can misclassify anomalies, leading to greater false positives and alert fatigue — something security teams are already struggling with. Hidden biases and errors in training data can create loopholes and vulnerabilities, allowing threat actors to exploit them. AI can create a false sense of security. Organizations may make the mistake of overlooking the ongoing need for hands-on employee training because they rely too heavily on machine automation.

Maintaining and monitoring AI systems is resource intensive. For AI to work properly, it must be fed massive amounts of data and collecting such data can be cost prohibitive. Attack vectors evolve so rapidly that retraining and updating AI models demands frequent cycles, which can stretch already limited security resources.

The need for human oversight, expertise and intuition

Like human skills, AI too has its limits. AI can automate routine tasks, but it’s certainly not at a stage where it can be trusted with making serious security decisions. This is because AI lacks the contextual understanding that humans naturally have for practical decision-making.

AI does not possess the human intuition called for detecting and preventing targeted social engineering attacks. AI will struggle to detect these attacks; that’s because scams can be tailored to individuals, using persuasive language [“free coupons!”] to deceive people into falling for phishing bait. Moreover, these attacks are conducted using legitimate channels (email, text, phone calls), making it challenging for AI-powered tools to sort the wheat from the chaff.

AI systems need human oversight. More than 90% of machine learning models degrade over time and deep learning algorithms are known to suffer a black box problem – the ironic failure of AI developers not fully understanding how AI “thinks”.

Moreover, AI is prone to exploitation and hacking. AI models can be injected with malicious training data; attackers can insert a backdoor that can be used to modify or weaponize the AI algorithm. Thus, human expertise is needed for monitoring the behavior and efficacy of AI models and to ensure safety and security.

Finally, there are cybersecurity elements that are beyond AI. For instance, organizations must build a culture of cybersecurity to mitigate human error because people are responsible for allowing most cyberattacks to prevail. A machine cannot be expected to build a rapport with people or get employees to conform and commit to following security best practices. One needs an empathetic touch, an intimate knowledge of social norms to connect, teach and empower people.

Using AI to fight cyber threats at scale is certainly the future. However, it will be a while before some autonomous AI can make individual security choices. Until then, organizations will need to persistently invest in education to develop the right skilled personnel to train and monitor AI systems. In concert with fostering a culture of security awareness, human intuition is needed for defending against sophisticated threats.

https://www.securitymagazine.com/articles/100378-ai-may-revolutionize-security-but-not-without-human-intuition