

“Sophisticated machine learning algorithms and predictive analytics are empowering organisations to better predict, identify, mitigate and neutralise cyber threats quickly

WWW.BETTERAI.IO



PROACTIVE SECURITY SYSTEMS

Merilee Kern discusses the value of AI in protecting the digital environment against cyber attacks



In today's world where cyber threats are becoming increasingly complex and downright relentless, the application of AI in cybersecurity strategies is a welcome advancement that helps us protect our digital environments.

Sophisticated machine learning algorithms and predictive analytics are empowering organisations to better predict, identify, mitigate and neutralise cyber threats quickly – and far more accurately.

“Cybersecurity is undergoing a para-

Merilee Kern (MBA) is an internationally regarded brand strategist and analyst. She is also the creator and host of the Savvy Ventures business TV show that airs on FOX Business TV and Bloomberg TV (she can be contacted at www.TheLuxeList.com and www.SavvyVentures.tv).



digm shift, transitioning from threat reaction to threat prediction and prevention,” says the Co-Founder and CEO of AI solutions developer BetterAI Angel Vossough.

She adds: “This change is set to be foundational to the industry, moving it toward security solutions that are more proactive than ever before.”

Here’s a deeper dive with Vossough into how artificial intelligence is enhancing

cybersecurity and safeguarding the collective digital landscape.

Q: What are some of the top line impacts that AI is having on the cybersecurity function?

A: For one, the incorporation of artificial intelligence into cybersecurity provides capabilities to detect and respond to active threats in real time.

AI is also able to learn from these threats and identify vulnerabilities in systems before they are exploited. These abilities drastically reduce the time taken to identify and mitigate current and potential security breaches.

Predictive security measures are already a longstanding aspect of modern cybersecurity practices. However, even the best human based techniques are unable to catch all potential vulnerabilities in systems of ever growing complexity and size.

AI is the next evolution in the cybersecurity arms race.

Q: In your view, what are some of the challenges faced when integrating AI into cybersecurity methods?

A: AI’s superhuman skill in pattern recognition and mass data processing enables it to sift through large amounts of data, and pinpoint threats that may go unnoticed by human analysts. Whether it’s detecting network intrusions, or analysing system behaviour to uncover vulnerabilities or malware, artificial intelligence has a critical role to play.

The need for AI in cybersecurity becomes even more pressing as cyber criminals are increasingly adopting artificial intelligence for their own malicious purposes.

However, the integration of AI into cybersecurity protocols presents its own set of challenges. Biases hidden within the black box of deep learning models have the potential to create a new set of blind spots that may be challenging to detect and correct.

For example, if an AI system is trained on data that predominantly features attacks from a specific geographic region, it may develop a bias that leads to a higher rate of false positives or negatives when analysing threats from other locations.

Additionally, it may have difficulty grasping the human motivations underlying certain cyber attacks such as political, ideological or personal factors that drive attackers.

This limitation may negatively impact artificial intelligence’s predictive capabilities, as it may not be able to anticipate attacks that deviate from purely technical or financial motivations.

Overcoming these obstacles calls for an effort that combines the enormous power of AI with the social awareness and technical expertise of human cybersecurity and machine learning professionals.

Q: Can you cite a few AI cybersecurity solutions that are evolving in this space?

A: The incorporation of artificial intelligence into cybersecurity solutions represents a major leap forward in addressing the constantly evolving cyber threat landscape.

We are already seeing AI cybersecurity tools such as NVIDIA’s Morpheus framework and IBM’s Security QRadar Suite hit the market.

Incorporating artificial intelligence into cybersecurity is not merely about improving the security posture.

It’s an essential step in protecting our digital environment from sophisticated threats. The future is here and the industry is undergoing a rapid change to adapt.

AI’s predictive capabilities enable organisations to proactively protect their networks and data from unauthorised access and exploitation.

As the industry increasingly adopts AI driven solutions, collaboration between artificial intelligence experts and cybersecurity professionals is essential for developing robust, transparent and responsible systems.

Only through this collaborative approach can its full potential be realised when creating a more secure digital environment for all concerned.

The incorporation of artificial intelligence is reshaping cybersecurity relative to the technology’s unparalleled ability to identify, address and rectify threats much more accurately and rapidly than ever before.

AI powered innovations are producing proactive and flexible cybersecurity systems that are capable of outpacing the ever-changing threats of the environment, and fostering a much safer digital landscape.

