Why Machine Learning & Human Intelligence Must Combine to Enhance Cybersecurity

Content

The future of cybersecurity

We're living in a time of great technological change, and driving the change is our increasingly connected world. In 2019, 4.39 billion people – 57% of the global population – were connected to the internet via an estimated 25 billion devices. Both numbers will continue to grow over the coming years. However, an unprecedented amount of connections raises a critical question: how do we keep all these connections secure?

Cybersecurity has always evolved alongside potential threats. But now the threats are evolving quicker, and unfortunately cybersecurity solutions are becoming outdated – fast. Existing solutions simply cannot scale at the necessary pace to offer meaningful protection.

You don't need to look far to see that this is the case. In the last year alone, Capital One (100 million affected customers), First American (885 million), Facebook (540 million), British Airways (500,000) and Marriott International (500 million) all suffered substantial data breaches on an unprecedented scale.

Traditional cybersecurity has been found lacking, but there is an answer: machine learning, the future of cybersecurity.

In this paper, we'll look at the rise of machine learning and why it holds the potential to reinvent how we approach cybersecurity. But we'll also show why machine learning on its own isn't a viable solution. Without an underlying data strategy and the aid of human intelligence, machine learning will be little more than a gimmick. Here, you'll learn why human intelligence must combine with machine learning to enhance cybersecurity for everyone's benefit.

Machine learning and the future of cybersecurity

Malware, ransomware, spear phishing, denial-of-service attacks – the sheer number of threat avenues available to hackers is awe-inspiring. But what is more jaw-dropping is the fact that threats are increasing. In an age where 25 billion devices are connected to the internet, over 360,000 new malicious files are detected every day. The number of threats is rising, especially as more people see opportunities for financial gain in cybercrime – businesses are predicted to have lost over $2.1 trillion by 2019 to cybercrime.

Traditional cybersecurity is outgunned. Conventionally, it has tried to protect against cybercrime via methods like signature-based and anomaly-based detection, but these methods either don't protect against new forms of attack or can flag too many false positive alarms. As the scale of threats increase, these methods aren't good enough. Cybersecurity specialists cannot introduce defences against threats fast enough. They simply don't have the physical endurance or brainpower to keep pace.

However, machine learning paves the way to a brighter future for cybersecurity.

What is machine learning?

Machine learning refers to an application of artificial intelligence (AI). It refers to machines that learn new skills or knowledge while processing large quantities of data. The machine can access and use data to learn autonomously, meaning the machine doesn't require human programming to acquire skills.

Why choose machine learning?

Right now, cybersecurity is trailing behind the complexity of threats because security solutions require human input to function. When new threats emerge, as hundreds of thousands do every day, to one degree or another it is a human being that must find a defence.

It's unrealistic to expect existing solutions to scale and offer the necessary levels of protection. Machine learning is the only answer.

With this new technology, businesses can train a machine to recognise possible threats to a system at lightning speed. To do this, businesses must feed machine learning applications with vast data so the machine can learn what a threat looks like and identify it. In addition, the machine will learn how to predict where vulnerabilities in the system reside and flag these issues.

Machine learning will soon become an indispensable tool in the IT and cybersecurity field. But there's something important to highlight here, namely what was touched on above: "businesses must feed machine learning applications with vast data".

Machine learning won't be the cure-all to cyberattacks, at least not on its own. It will need a human's help to fulfil its potential. It will need a robust data strategy.

The Wizard of Oz: Data Strategies

One of the most famous computer programming principles is: garbage in, garbage out.

This principle refers to the idea that a computer program is only as good as the data you provide it with. If you provide poor data, you'll get poor results. But if you provide great specialist data, you'll get spectacular results.

Such is the case with machine learning. These AI applications learn from the data that humans provide it with. If we gather and provide poor, unrepresentative or incorrect data, the machine won't be able to spot or predict threats accurately.

It's vital that businesses hoping to capitalise on machine learning's possibilities invest in data scientists. These are the people who will feed your machine with the data it needs to perform its activities.

As an integral part of the team, data scientists will probe businesses to acquire the data the machine needs. It will be the data scientist's responsibility to select the right data for the job. That doesn't just mean knowing what the right data might look like but, knowing how to ask the right questions to get the best data out of the team.

In the end, data scientists have to act as a kind of Wizard of Oz. If you were to pull back the machine learning curtain, you would find a data scientist charting a data strategy. As Ken Durazzo, a vice president for technology research and innovation at Dell Technologies, said, these Wizards of Oz must ask themselves "what data do I need to help the machine understand what it should know and what it needs to process and get to the outcome set I'm looking for."

But although humans will need to teach new cybersecurity machines what to look out for, that won't be the only thing machine learning will need humans for. Businesses must look at machine learning not as a panacea but as an extra, formidable tool for IT and cybersecurity teams to wield.

A match made in heaven: Human intelligence & machine learning

In 1996, chess world champion Garry Kasparov lost at chess to IBM's Deep Blue supercomputer. It was a landmark in AI development, and plenty of people thought it spelled the dawn of intelligent machines.

It was an impressive feat, but it is important not to get carried away. Deep Blue was able to evaluate 200 million positions per second, which it would rank in order of probability for delivering a win. This made Deep Blue astounding at chess. However, Deep Blue was only good at chess. It had no other skills or experience to draw upon, meaning that it couldn't approach chess in a creative way. Arguably, Deep Blue did make some inspired moves, but the jury is still out on that one and whether it had an overarching strategy either is up for debate.

That isn't the case when it comes to humans. A human being has a wealth of experience to draw upon, gained from living a full life out in the world. They can have multiple skills covering a wide array of topics, and these experiences can promote greater creativity in other, unrelated areas.

Empathy is another crucial human trait; a human being can appreciate the nuances of human behaviour and imagine scenarios with another human, like how criminals might use new technologies to find new ways to commit crimes like ransom, burglary, and fraud.

It is because of this that machine learning will only be as good as the employee who wields it. After all, machines can make mistakes, as the example of Stanislav Petrov in 1983 suggests. Many people regard Petrov as 'the man who single-handedly saved the world from nuclear war' after he believed an alert of nuclear attack from the US was a false positive. Petrov questioned the machine's interpretation of events and thus exposed a flaw in the alert system.

It will be the same with machine learning, at least for the foreseeable future. The machines will be able to break down the vast range of possible threats to identify and provide ranked probabilities for the few that could be a real threat. But ultimately it will take a human being to confirm and retaliate to these threats.

From a data standpoint, humans bring the qualitative insights while machines can analyse quantitative data. These are two sides of the same coin, with both qualitative and quantitative analysis needed in the fight against cybercrime. As such, in the future machine learning and human intelligence must combine to enhance cybersecurity.

This match made in heaven will work because machines require accurate, relevant data sets to learn how to protect systems from cybercrime – something humans can and must provide. On the other hand, humans don't have the physical endurance or brainpower to sift through myriad cyber threats – something machines can do with ease.

By taking the scalability and pattern-spotting capabilities of a machine and pairing it with the intuitive intelligence of a human being, the world stands to benefit from a more secure digital environment.

Transforming cybersecurity with ML

The future of cybersecurity will be a far cry from where we are today. There will be a closer partnership between human and machine to provide a solid defence against cybercrime, with machines taking the role of trusted advisor to the cybersecurity specialist.

By utilising this new tool, security specialists will be able to scale their protection of an organisation's systems to meet the realities of the modern digital world head on.

The onus is now on organisations to invest in machine learning, data scientists and cybersecurity specialists to ensure they are fully protected from the threats of tomorrow.

To start your own cybersecurity transformation, here are a few tips to begin your journey:

Audit your systems to understand how machine learning can help plug vulnerabilities in your system and scale to the level of threats

Invest in a data scientist today to start collating the right data sets and data strategy your ML will need to adequately protect your organisation

Break down the siloes between your teams to acquire more relevant, accurate data to teach to your machine

Review your security processes to ensure that that when your ML goes live, possible threats can be reviewed and acted upon quickly

Why Machine Learning & Human Intelligence Must Combine to Enhance Cybersecurity

CEO.digital is the digital transformation hub for C-level, Directors, Heads and senior executives. We create, publish and promote future-focused content independently and in partnership with global brands.

Dell Technologies is a US multinational computer technology company that develops, sells, repairs, and supports computers and related products and services. the company is one of the largest technological corporations in the world.

YOU CAN FIND MORE DIGITAL TRANSFORMATION REPORTS AT CEO.DIGITAL