

# AI, machine learning boost cybersecurity

The last few years have seen a massive rise in the number of data breaches affecting major organisations. Alongside this, security challenges are changing fast. Pimpily hackers in basements have morphed into sophisticated criminal networks, and viruses have turned into advanced persistent threats.

The attack surface and number of entry points have proliferated exponentially. Security incidents are now an inevitability, and focus has turned from trying to prevent breaches to identifying and remediating attacks as fast as possible to limit the fallout.

“The changing nature of the security game is seeing a number of trends rise to the fore,” says Simon Campbell-Young, MD of Credence Security.



Simon Campbell-Young, MD of Credence Security

Firstly, he says privacy and personal data protection will continue to be a major focus in 2018. Ever since the Protection of Personal Information (PoPI) Act was signed into law, businesses of every type and size are under the obligation to prepare themselves. “Businesses need to become PoPI compliant immediately, which will have massive implications not only for their policies but on how they enable these new processes and ensure that they are implemented effectively throughout the business.”

Multinationals that are based in South Africa will also have to think about data regulations in other countries, such as the

General Data Protection Regulation (GDPR) which will have a significant impact on them, and the way they handle and store their data.

### **Rise in AI and machine learning**

Next, he says we will see a rise in machine learning and AI being used for cybersecurity. “In the context of information security, AI is a tool that understands its environment well enough to pinpoint events and take action against a predefined purpose. AI is exceptionally good at recognising patterns, and therefore anomalous behaviours, making it a superb tool for threat detection.”

Moreover, Campbell-Young says that with businesses under pressure to save money and hiring pretty much frozen across the board, organisations are turning to machine learning and AI to automate resource-heavy tasks that would have taken staff away from their core functions.

“And hand in hand with AI comes machine learning. This is essentially software that can learn on its own based on human input and results of actions taken. In conjunction with AI, machine learning can become a tool to predict future outcomes based on the events of the past.”

He says to remember that these tools can scrutinise multiple actions and massive amounts of data in a fraction of the time it would take even a team of people. These technologies can look for indicators of compromise across the entire network, on premises, as well as in the cloud.

### **A rise in customised security solutions**

Campbell-Young believes there will also be a rise in terms of customised security solutions. “As the threat landscape evolves, and companies face a slew of increasingly cunning and sophisticated attackers, organisations are waking up to the fact that security isn’t a ‘one size fits all’ solution. There is a big disconnect between organisations and effective security measures. Just because a solution is ranked as ‘best-in-class’ doesn’t mean it’s necessarily right for your company’s specific needs.”

He says companies are realising they need to add different security tools or layers, based on their individual needs. “Others are looking for customised solutions to meet their unique security challenges, or are building in-house capabilities to meet these requirements. Each business and industry is different, as are their security needs. I definitely see businesses investing more heavily in localised solutions and products, to fulfil requirements that traditional solutions simply can’t meet.”

The last decade has been a tumultuous one in terms of cybersecurity. The number and frequency of attacks will only increase, and they will become more targeted in nature. Businesses will have to do more with less and will need to adopt approaches to cybersecurity that help them protect their critical business data without hampering innovation and growth.

For more, visit: <https://www.bizcommunity.com>