MACHINE LEARNING

Tim Wallen *discusses what is needed to lay the foundations for the success of next-gen cybersecurity technologies.*

The expanding scope and sophistication of cybercrime is a significant problem. When we hear the word 'cybercriminal', there's a tendency to picture a single individual hidden away in a dark dingy garage, operating from an old-school laptop. And while this may have once been the case, modern cybercrime looks entirely different.

Today we're faced with incredibly organised and highly sophisticated criminal operations backed by vast resources and often nation states. It is these networks that are intensifying the threat landscape, making cybercrime a much more real, fierce danger to organisations of all shapes and sizes around the world. You only have to glance at some statistics from 2021 to get a sense of the bigger picture.

According to IBM, the average cost of a data breach rose to $4.24 million in 2021 – the highest this figure has been for 17 years. Meanwhile, further research also shows that corporate networks saw a 50 percent increase in attacks per week when compared with 2020. Given the uptick in both the volume of attacks and associated damages, it should come as little surprise that a leading US insurance company paid out a record $40-million ransom last year after attackers stole the firm's data and blocked access to its network.

We're starting to see the true power of RPA and AI in predicting when and where attacks might happen

The unfortunate reality is that cybercriminals are continuing to be successful in their efforts, creating a snowball effect that is fuelling the determination of threat actors to innovate their attack methods in an attempt to secure lucrative rewards.

Resultantly, unprecedented pressures are being placed on cybersecurity professionals at a time when the sector is struggling with a severe skills deficit. Indeed, one report estimates that the number of unfilled cybersecurity positions grew from one million in 2013 to 3.5 million in 2021. Within this context, cybersecurity is always fighting an uphill battle. Attacks continue to come thick and fast and security professionals are forced to scramble in order to protect their systems wherever possible, forever playing catch up. Of course, this isn't a sustainable way to operate. It just takes one successful attempt for threat actors to succeed, and – operating under such stressful circumstances – security teams will sooner or later slip up.

Fortunately, to the benefit of many industries, technologies are beginning to mature and are now showing their potential in turning the tide in the fight against cybercrime. We're starting to see the true power of robotic process automation (RPA), machine learning and AI, not only in providing real-time insights but also in predicting when and where attacks might happen.

There is an argument to say that such technologies will be the only way to keep pace and counter the ever-changing methods of cybercriminals. It's not enough just to detect incidents anymore. Instead, a holistic approach is needed, and these advanced solutions are critical to achieving that.

Through AI and machine learning, automated threat detection and response can be achieved, taking much of the pressure off security teams in spotting and acting upon threats and incidents. Leveraging these technologies allows security teams to be fully armed and forewarned, facilitating transparency, enhancing clarity and reducing the potential for panic in critical moments. In other words, they can make security a much smoother, more seamless operation.

The old adage 'time is money' is never truer than in a security sense. Using automation, security professionals can dramatically reduce the time taken to not only detect but equally deal with a threat – and in turn save significant sums induced by downtime, ransomware demands or the many other adverse effects of an attack. Further, these technologies don't just save money. They also drive down costs in a proactive manner.

Right now, solution saturation is a huge issue plaguing the cybersecurity market, with reports showing that companies may have up to 70 different security vendors installed at any one time. In such instances, many overlapping solutions might be running simultaneously that paint a complex picture, leaving organisations incapable of determining which of their many tools are providing actual value and which are not.

Historically, security investments have been reactionary and, therefore, immediate. When a firm may realise it has a gap, they plug it by investing in tools that are built for that specific purpose. However, over time this approach can create inefficiencies. You can end up with two or three technologies that are all doing the same thing. If one of those is effective 99 percent of the time, organisations should be able to ask themselves if they need those other two technologies to deal with the one percent, and if that's worth it for the price.

Automated analytics and correlation technologies can provide key insights here. Using data, they can determine when one technology covers all bases and if the two are simply not needed, helping firms to minimise their operational overheads with meaningful automation.

In security, human-driven detection and response and automated detection and response are night and day. If done right, the latter can deliver a host of benefits, be it cost efficiencies or improved transparency of operations. However, there is a catch. Machine learning models aren't a case of plug-and-play. There are many factors influencing the effectiveness of these technologies, and companies need to create the solid, comprehensive foundations from which they can thrive.

A critical issue here is the availability and reliability of data that is being used to teach machine learning models. Are there any external data sources that can be cross correlated with? How many do you have access to? What's the bias on those data sources? If you're only taking a small subsection of data, your machine learning models will fail to have the adequate information needed to develop adequate intelligence and in turn, power accurate and informed actions. Companies therefore need to consider ways in which they can expand their datasets and, in effect, begin to develop and run a data lake – even if it's just for security purposes.

THE AVERAGE COST OF A DATA BREACH WAS $4.24 MILLION IN 2021 – THE HIGHEST FOR 17 YEARS

This data lake should include mapping users. For machine learning to truly work in a security context, you need to understand what your users are doing, what applications they use, at what times and in what ways. This will ensure that anomalous activities can be spotted immediately, triggering an automated response.

Without trying to sound like a broken record, this requires patience. For intelligence to really understand and prioritise whether certain anomalous activities are a genuine risk to an organisation, a lot of history and a lot of data points are required. This simply needs to be accounted for – much like an employee, if we give a machine learning model just 30 days to get 100 percent up to speed, it is simply not going to happen. Companies must start slowly and treat these technologies as if they are a new starter, rather than expecting them to deliver overnight.

Given this opportunity, machine learning and AI can become game-changing weapons in the fight against cybercrime – yet providing this environment may require a mindset shift. Firm's need to shift from being policy-led to data-led. Indeed, policy remains a critical component, helping dramatically in achieving compliance and ordering the operating environment, but given the current threat landscape, security decision-making must be data-driven.

Internal data generated by everything from user activity to threat feeds can provide critical insights, showcasing where a company may or may not be vulnerable. Most organisations will have this data – whether they're listening to it, or have the ability to interpret it, is another matter. Companies need to have a way to visualise their data easily. Only then can they start to tap into the power of automation. It is for this reason that AI presents a quantum leap forward.

Moving from detect and response security protocols that rely on human cognition to a fully automated security posture is a major jump and may involve the leapfrogging of many technologies in between. It is a process that might seem a little overwhelming, but with a data-led mindset it won't be difficult to achieve. It is easier today than ever before to take this quantum leap into automated detection and response, and many larger firms are already on this pathway and talking in these terms, building data lakes and incorporating AI and machine learning.

AUTOMATED THREAT DETECTION AND RESPONSE REDUCES THE PRESSURE ON SECURITY TEAMS

In the grand scheme of security, having complete visibility of an organisation's network and an appropriate response for any given threat level is a vital step to take. To deal with sophisticated threats, security responses need to be dynamic to be effective. In order to achieve this, we need to leverage cutting-edge technologies and, therefore, need effective data-led foundations.

So, what can we expect for 2022? As the effectiveness of AI, machine learning and RPA technologies continue to come into greater focus, I anticipate that firms will begin to iron out additional issues that will further enhance security ecosystems. We are seeing obstacles now in regard to partner technology, so interoperability is perhaps the next big hurdle that needs to be overcome.

Further, the mass shift to the cloud that we have witnessed during the pandemic has also complicated security for many companies where migrations may have created blind spots. While the cloud is undoubtedly the future – a key technology in which flexible and hybrid working models can be built, unlocking a host of operational benefits and efficiencies – security teams are now tasked with ensuring that hybrid environments are as secure as the on-prem environment was.

Simply put, the perimeter doesn't exist any more. That's a reality that we're still navigating, with users interfacing and accessing data in different ways. As an example, it's led to the introduction of new policies such as zero-trust and questions surrounding authentication. If you're talking about intelligence, intelligence needs access, so how do you trust your intelligence engine to have access to everything if there's no trust by design? With these developments and considerations, the landscape has undoubtedly become a bit more complicated.

Yet security teams still need to monitor activities and make informed, logical decisions. Therefore, just as the cloud has become a critical component in improving the effectiveness of company operations, machine learning must equally become a vital pillar of security. If it does, and in the right way, then a massive burden will be lifted from security teams and the resulting benefits will be numerous ●

Tim Wallen is Regional Director UK&I, LogPoint

Automated analytics and correlation technologies can help firms to minimise their operational overheads