Cybersecurity risks: the benefits of Machine Learning and UEBA (User Entity Behaviour Analytics)

By Doros Hadjizenonos, Regional Director – SADC at Fortinet

The cost of cybercrime is rapidly outpacing our ability to keep up. While Gartner predicts worldwide spending on Information Security to reach $124 billion this year, security researchers also estimate that the cost of cybercrime will exceed $2 trillion in that same time, outpacing security spending by over 16X.

The vast majority of malware simply targets known vulnerabilities, while botnets now remain undetected inside targeted organisations for an average of nearly 12 days. The problem in many cases is one of resources. The rapid expansion of the attack surface through digital transformation and the unprecedented adoption of BYOD and IoT devices, combined with the growing sophistication of attacks and widening security skills gap has overwhelmed many security teams.

To address this challenge, organisations are turning to things like Machine Learning (ML) to fill their security gaps. The question is whether machine learning can add new value to the realm of cybersecurity?

Detection and prevention of cybersecurity solutions

Most organisations are currently operating with the standard cybersecurity kit. Their wiring closets are filled with devices that tout security policies that vendors claim can detect and prevent the latest threats by way of signature-based detection, canned policies, or even user-defined configurations. Sensors in this category—and experts estimate that organisations may have solutions from as many as 70 different security vendors inside their network— include firewalls, data loss prevention (DLP) systems, intrusion prevention systems (IPS) and web content filters (WCF).

In addition, many of these devices operate in complete isolation, unable to share or correlate threat intelligence or respond to threats in any sort of cohesive or coordinated strategy. As a result, even monitoring these appliances requires an extra layer of sensors—along with additional security team members to manage them and hand-correlate their syslog events.

Machine learning - what it is

Machine learning (ML) is a subset of AI. AI and ML can augment our human capabilities by allowing us to carve through large datasets and spot patterns of behaviour, or signals in the noise, that would be all but impossible for humans to do. This provides a force multiple, enabling your existing human talent to spot unusual behaviour automated behavioural analytics, or UEBA (user entity behaviour analytics) tools. Mundane tasks can also be automated with ML, allowing scarce cybersecurity personnel resources to focus on higher value tasks.

User Entity Behaviour Analytics—providing the big picture

ML and AI are based on ‘big data’, and their efficiency and accuracy gets better the more data you throw at them. What’s important, however, is that you are collecting the right data. That’s where UEBA systems come in. Combining accurate and essential user behavioural data with machine learning allows you to more accurately monitor your users on an endpoint-by-endpoint basis, providing you with deep visibility into what they get up to on a regular basis.

Once a baseline of normal behaviour is established, any time a user does something that the UEBA system considers outside of normal, the cybersecurity ops team is alerted. If a user’s legitimate activity is flagged as anomalous, which can happen frequently during the initial learning stages, your analysts can simply tag the activity as routine and the UEBA system’s machine learning integrates that data and goes back to business as usual. As machine learning reduces such false positives, any time a user strays from normal behaviour those notifications become more urgent.

The benefits of combining machine learning with UEBA

Using machine learning alongside user behaviour data provides a level of security proactivity that is not possible when relying on traditional signature-based prevention and detection systems. This is due to the fact that you’re able to detect subtle changes in behaviour that’s tough to do with signatures. It’s simply not possible to configure a system with every single rule permutation to detect all attacks

Detecting low-level reconnaissance activity using UEBA and machine learning is far more likely to set off your Spidey-senses than combining machine learning with traditional signature-based detection measures. This provides a huge advantage, making it a lot harder for attackers to circumvent control by flying under any rules-based radar.

Conclusion

The benefits to using a UEBA security solution built on a machine learning platform are many. As their ability to baseline network activity is refined, they can not only detect anomalous changes in behaviour, but that information can also enable proactivity by identifying and preventing certain behaviours before the occur. And since machine learning solutions generally provide their own care and feeding, minus a few tweaks here and there, overhead to manage them is reduced to a minimum.

But perhaps most importantly, machine learning is coming on the scene at a very opportune time because the number of analysts required to sift through data by hand to identify threats is rapidly outpacing the number of professionals currently available. By removing the human from a task that they’re not especially suited to, they are free to focus on those areas where they can add value, such as further developing your cybersecurity practice.

So, does machine learning add value to cybersecurity? We’re going to go with yes.