Staying ahead of the race: AI & cyber skills to track online criminals

Detection capabilities have evolved, with alerts incoming with increased frequency. Here, Matt Walmsley, EMEA director of Vectra discusses how a skills shortage means greater opportunity for AI.

The number of threats that organisations are being subjected to is increasing exponentially. As a result, security incident response (IR) teams are being faced with an unprecedented dilemma. Once acting as a reactive, first line of defence against threats flagged by operational units within the organisation, IR teams and their skillsets are evolving to become proactive and preventative, with an emphasis on threat discovery.

Centralised event log collection, network traffic archiving, the creation of "data lakes," and a plethora of query and inspection tools have become the new focus for IR teams. They are embracing threat hunting methodologies and employing the latest data mining tools in an attempt to identify threats in motion and reduce threat discovery and response times. The objective is to intervene early in attack lifecycles before serious damage occurs.

Most senior IR specialists, experienced as they are in evidence gathering and picking through events at a byte-level, have broadly welcomed these new tools. However, the nature of the task is taking its toll as they are increasingly finding themselves being drawn thin on the ground.

In the past, a threat had often already exploded into a full-blown breach before it was noticed, and usually first by the affected business unit or, even worse, an external party. Yet, the stakes have grown so much in the past few years that organisations can no longer afford to let a suspected threat snowball into a successful attack before action is taken.

As a result, IR teams are being stretched beyond capacity as the speed at which initially suspect anomalies are detected outpaces their ability to deep-dive, validate and investigate the root cause. Detection capabilities have grown so much that now there is a tsunami of event alerts, some of which may contain suspicious events, generated each hour. The need to detect threats early on has forced many IR specialists to abandon their traditional investigative and forensic techniques. In such a high-stress environment, mistakes will happen and red flags missed.

With the EU's General Data Protection Regulation (GDPR) on the horizon, these challenges will weigh on the minds of many organisations. Alongside the reputational damage that usually follows a breach, GDPR can make the consequences of a data breach economically devastating if a maximum fine is levied.

> "LEVERAGING THE LATEST TECHNOLOGIES, SUCH AS MACHINE LEARNING AND ADVANCED BEHAVIOURAL ANALYTICS, THEY CAN TAKE THE WEIGHT OFF EXISTING STAFF AND AUTOMATE THE TRACKING OF AN ATTACKER'S ACTIVITIES INSIDE A NETWORK BEFORE AN ATTACK CAN WREAK HAVOC."

How then does an organisation retain or justify its need for experienced, senior tier-3 specialists? These artisan employees offer many years of cybersecurity experience combined with a rare understanding of the business's context. Yet, when their primary role involves time-consuming entry-level work such as data-mining and false-positive triaging, their core skills are wasted. This can actually become a disincentive to stay, particularly in today's employment market where their talents are always in demand.

Too many organisations have persisted in the belief that they can redirect their senior IR professionals, who would then willingly remain in these new roles. The result has been the opposite. In the UK, there are twice the number of open cybersecurity positions than there are certified professionals to fill them. This is particularly acute at the upper end of the scale, and such policies have led to the disenfranchisement of technical leaders and exacerbated the drought of crucial, deep technical skills.

Organisations should wake up to the potential of Artificial Intelligence (AI) to reverse their fortunes. The latest generation of AI-enabled threat hunting platforms excel at mining the growing lakes of logs and alerts. These platforms can automatically correlate events and anomalies, categorising and labelling attacks in progress. Indeed, they have the potential to automate and replace entry-level incident analyst and responder roles entirely.

This should not be feared, but embraced. The automation of tier-1 security investigation tasks will readdress the critical workload balance many specialists struggle

with. Instead, these new platforms will allow the most experienced IR teams to work more closely with the business to address prioritised critical outlier events.

Outlier alerts occur when anomalous behaviours are picked up that are not obviously malicious. They often require a specific and intimate knowledge of the business to resolve – including the ability to contextualise when a large transfer of data is suspicious or routine. They also necessitate extracting evidence not typically captured in logs or alert events, all of which are metadata, not the primary evidence. Despite their challenges, outlier events keep highly valuable and skilled experts occupied, motivated and able to continually add value to the organisation.

However, the impetus for change should not fall solely on business. The public sector has often been exposed as equally guilty of failing to protect the data, systems and experts under its care. Ultimately, those responsible for key infrastructure must realise that traditional perimeter defences are not enough. Leveraging the latest technologies, such as machine learning and advanced behavioural analytics, they can take the weight off existing staff and automate the tracking of an attacker's activities inside a network before an attack can wreak havoc.

Conclusion

Greater use of AI technology will make a considerable contribution to bridging the cyber skills gap, adding capabilities that will take pressure off existing staff and improve their ability to respond to incidents and risk. The application of AI to cybersecurity is already providing an invaluable level of automation in entry-level security roles where the talent pool is dwindling. The technology can also be used to augment existing, high-value security specialists. Free from time-consuming entry-level roles, a company's top tier specialists are free to focus on what they do best.

For the foreseeable future, humans and AI are destined to work in synergy.

Matt Walmsey, EMEA Director, Vectra

The New Camera Line Mx6 Creates More Possibilities.
More Images, in All Light Conditions, in Every Standard.

More Intelligence Is on the Way.

The new Mx6 6MP camera system from MOBOTIX offers increased performance.

A frame rate that is up to twice as fast than that of other cameras allows it to capture quick movements even better and simultaneously deliver sharp images in MxPEG, MJPEG and, for the first time in H.264, the industry standard. The innovative Mx6 camera line is faster, more flexible and higher-performing, opening up new application and integration opportunities for to you to meet all requirements.

MOBOTIX AG • Langmeil, Germany • www.mobotix.com

MOBOTIX