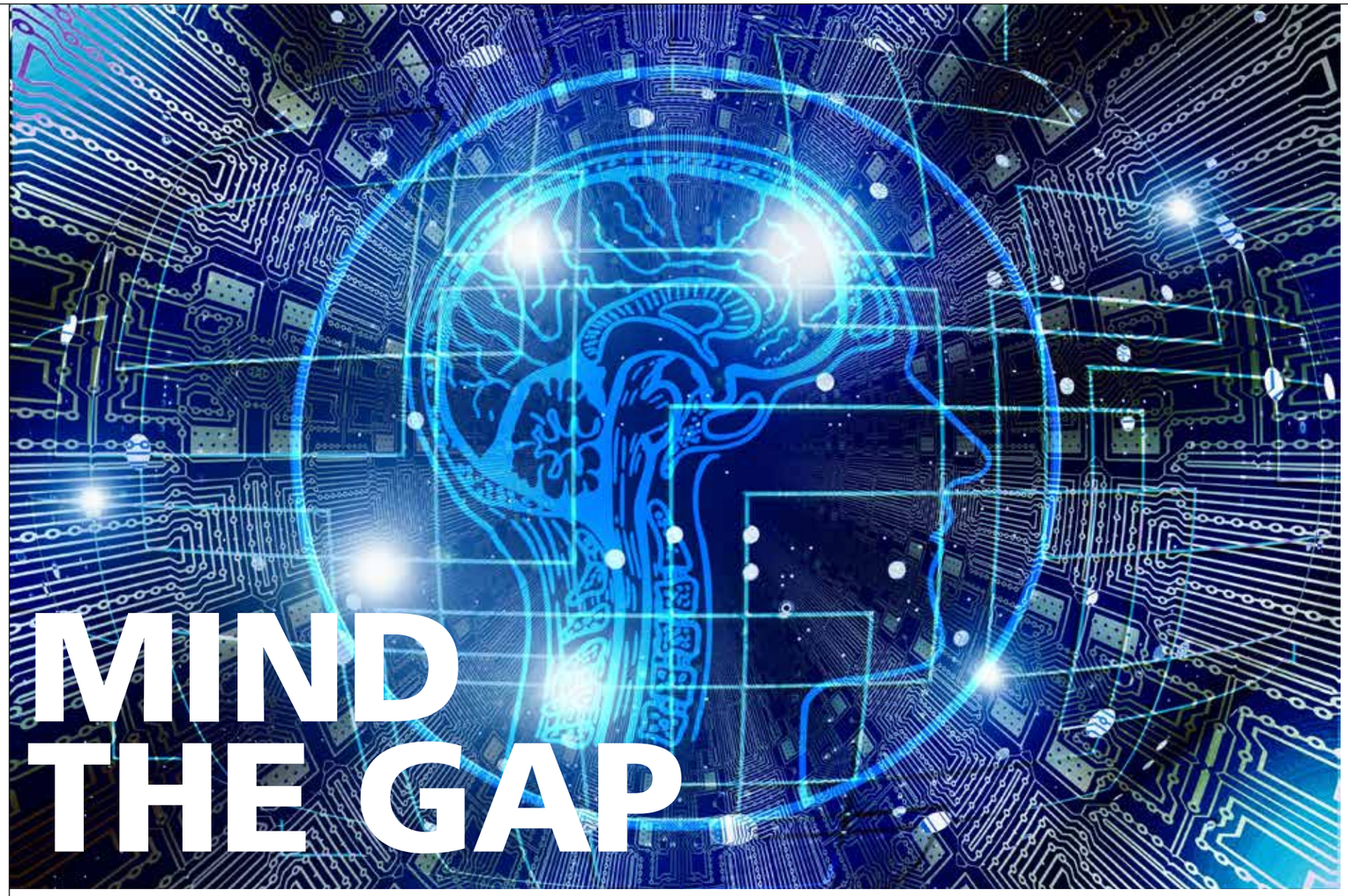

MIND THE GAP

Tim Wallen *discusses whether or not technology can plug the cyber skills gap*

Enterprises looking to attract and retain cybersecurity staff have a challenge on their hands in 2023. ISC² estimates that the global cybersecurity workforce became 4.7-million strong at the end of 2022, inflating 11.1 percent with the addition of 464,000 newly employed security professionals. However, despite this, the cybersecurity workforce gap actually expanded last year, growing at more than twice the rate of the workforce with a 26.2 percent increase year-over-year.

The industry is now faced with the mountainous task of bridging a worldwide gap of 3.4-million cybersecurity workers if cross-industrial enterprises are to be properly protected from modern cyber threats.

In the UK alone, the Department for Digital, Culture, Media and Sport (DCMS) estimates that approximately 697,000 businesses (51 percent) have a basic skills gap. In other words, the people responsible for cybersecurity within those organisations both lack the confidence to carry out the tasks outlined in the government-endorsed Cyber Essentials scheme and aren't getting adequate support from external security providers.

As you might expect, one impact of these skills shortages is an increased susceptibility to breaches. Fortinet's 2022 Cybersecurity Skills Gap Research Report shows that eight in 10 organisations have suffered from at least one breach that could have been avoided with better cybersecurity skills and/or awareness.

Given the potential impacts of breaches, this is a major problem. IBM's *Cost of a Data Breach Report 2022* shows that the average total cost of a data breach reached an all-time high $4.35-million last year – a figure that tallies up with Fortinet's analysis, which reveals that a staggering 38 percent of enterprises reported breaches that cost them more than a million dollars to remediate.

Unfortunately, the impacts that come with having inadequate cyber skills aren't solely financial. One independent study has shown that more than half of office workers would actually reconsider working for an organisation that had fallen victim to an attack, with only one in three saying they would be unfazed. In this sense, incidents can be so disconcerting that they may exacerbate staff turnover, creating a vicious cycle that sees resource further depleted.

While AI isn't likely to fully replace cybersecurity workers, automating consistent and repeatable processes can free them up to focus on higher value tasks

These financial and mental strains are only expected to worsen moving forward. At present, we're not seeing the flow through required to tackle the cyber skills gap effectively. According to the DCMS, there were 4,400 core cyber security postings each month in 2021 – an uptick of 58 percent on 2020 averages. And while there have been roughly 7,500 new entrants into the cyber security labour market each year, there have also been about 4,600 people leaving the profession. For this reason, it is estimated that we're currently experiencing an annual shortfall in cyber security personnel of more than 14,000 in the UK alone.

Any idea that we can simply "ride out" the skills gap is unrealistic. Something needs to change – without action, the current skills crisis will only continue to get worse and worse year after year, placing ever greater strains on already limited cyber resources.

Organisations should therefore work to support their security teams wherever they can, enhancing their toolkits and empowering them to work in the most effective and efficient manner possible. Here, technologies can help. While AI isn't likely to take the place of cybersecurity workers any time soon, automating consistent and repeatable processes can free up workers to focus on higher value tasks.

With the right solutions, firms can take the pressure off security teams, helping them work more productively while improving their overall employee experience. Not only will this make it easier to retain talent, but it can also serve to reduce staffing shortages without requiring additional staff.

So, exactly where and how should enterprises leverage automation to the benefit of security? This is a question to which the answer must be very carefully considered. While it can be tempting to acquire every shiny new solution under the sun, such an approach can do more harm than good.

More doesn't always mean better. An expansive range of automated solutions will cost a lot, and that's not going to be desirable or sustainable for many firms given the current economic climate. Equally, it can make the lives of security professionals that need to learn to navigate all these various applications more complex. Furthermore, many solutions can become redundant, duplicating capabilities, while the need to manage multiple platforms will contribute to alert fatigue.

Instead, organisations should work to optimise their security support network by ensuring the logical convergence of technologies that accelerate detection and response by fusing telemetry and automating responses across the enterprise technology stack.

Security professionals need to be supported with platforms that provide efficiencies of scale to help build defensive capabilities. Any technologies should therefore empower them by providing a comprehensive overview from which cyber threats can be managed and business risk reduced.

That might be achieved by surfacing high-value true positives and providing threat context to prioritised cases, or by providing data to optimise the efficacy of the broader security infrastructure. Above all, these solutions need to be easy to use, freeing up security personnel to focus on solving genuine cyber security issues.

There are several technologies that should form central pillars of the automated technology stack, user and entity behaviour analytics (UEBA) being a prime example.

Using advanced machine learning, UEBA works by building baselines for normal behaviour for every user, peer group, and entity in a corporate network, instead of applying predefined rules for standard behaviours. In doing so, UEBA is then able to identify activity that strays away from these baselines to detect abnormal and risky behaviours which may not be immediately obvious otherwise.

It is a technology capable of providing tailored detection to each user, so that analysts can spot, prioritise and manage anomalies easier. Indeed, with UEBA, analysts are able to accelerate threat hunting with capabilities that serve to reduce alert fatigue and drive professionals to focus on those threats that genuinely require remediation. As a result, UEBA can provide vital support in mitigating risks, damages and data loss incidents by eliminating false positives and cutting down response times significantly.

THE INDUSTRY NEEDS TO BRIDGE A WORLDWIDE GAP OF 3.4-MILLION CYBERSECURITY WORKERS

Alongside UEBA, security operations centres should also tap into threat intelligence to add context to alerts and improve outcomes.

Successful security relies upon the ability of organisations to understand their vulnerabilities and deploy adequate knowledge and intelligence to mitigate potential threats. While indicators of real risk are often difficult to identify, and preparation for every single new threat is impossible, making the best use out of the intelligence sources that are available can help security professionals to prioritise threats and broaden their armouries.

Threat intelligence automation can be used to achieve this, enabling organisations to collect and analyse data on the latest threats. Be it security vendors, intelligence groups or other connections, leveraging information from a wide range of sources can help in proactively identifying trends and initiating security activities to stop malicious behaviour and avoid incidents.

It is a means of logically informing security decision making. By combining intelligence and previous experiences from many organisations into a single, central feed, security teams can make better strategic choices to help mitigate attacks.

Of course, manually trying to identify threats within large volumes of collected information can feel like finding a needle in a haystack. For this reason, automation is key. Analysts should automate event interrogation, screening hundreds of thousands of indicators of compromise (IOCs) across a variety of internal and external intelligence feeds to evaluate the data based on known attacks. In doing so, they can benefit from an accelerated ability to correlate multiple threat indicators generated inside their perimeter with external threat IOCs.

In addition, security teams should also look to embrace security orchestration, automation and response (SOAR). SOAR is all about alert aggregation and prioritisation. It's an incident detection and response technology centred around workflow and playbook

automation that accelerates threat investigation and remediation by guiding analysts towards consistent and optimal responses.

By automatically pulling all cyber incidents and supporting data together in one place, it can provide structured workflows for day-to-day security analyst tasks, serving to decrease response times and helping analysts identify and resolve incidents fast. Through correlating and analysing data, SOAR can present all contextual information and intelligence, allowing security teams to react more efficiently and effectively. Not only can this help to improve productivity, with SOAR capable of recommending a response so analysts can simply approve or execute a decision, but it can also reduce alert fatigue and information overload.

8 IN 10 ORGANISATIONS HAVE SUFFERED FROM A BREACH THAT COULD HAVE BEEN AVOIDED

Without question, solutions such as UEBA, threat intelligence automation and SOAR can help organisations to bridge the cyber skills gaps by empowering security professionals and in the process freeing them up to focus on additional high-value tasks.

Encouragingly, organisations are beginning to recognise these merits. Indeed, automation is becoming increasingly prevalent in cyber security, with 57 percent of firms having already adopted it and an additional 26 percent planning to do so in the future. However, businesses planning to invest in such technologies must plan wisely, particularly in light of current economic conditions.

According to Gartner's 2022 Board of Directors Survey, business leaders now acknowledge that security incidents can have significant impacts on an organisation – so much so, that 88 percent of boards now consider cybersecurity a business risk, this up from 58 percent five years ago. This is positive, but professionals must still invest wisely. Any strategic failures could serve to undermine this newfound appreciation of security, so firms need to be cost-effective in their methods while also improving performance – ideally with no mistakes.

With this context and the needs of modern security professionals in mind, embracing a converged security solution makes sense. Enabling organisations to combine multiple tools into one platform, converged solutions can reduce the number of point solutions and vendors that security teams need to manage. This is key, as complexity in IT departments is typically driven by integrations, technology evolution and changes to scope. Therefore, selecting a solution with a broad set of features limits complexity, cost and friction.

Performance can improve too. By combining SIEM centralised monitoring with automation, workflows and a case management system, all in one tool, security teams can benefit from all the necessary data to support better outcomes.

Not only does this cover all bases to give peace of mind, but it also offers transparency into total cost of ownership. A sound converged security setup will offer a predictable licensing model that is dependent on factors that are within the customer's control, so they know exactly what they are getting for their money. Looking ahead, it's this convergence that promises to be the real gamechanger in helping businesses navigate the cyber skills gap ●

Tim Wallen is Regional Director for the UK&I at LogPoint. With almost 20 years of cybersecurity experience, he has held senior sales and management positions within both high-growth and established vendors, including FireMon, ForeScout, Check Point, McAfee and IBM.

The Department for Digital, Culture, Media and Sport estimates that 51 percent of UK businesses have a basic skills gap

Picture credit: Logpoint