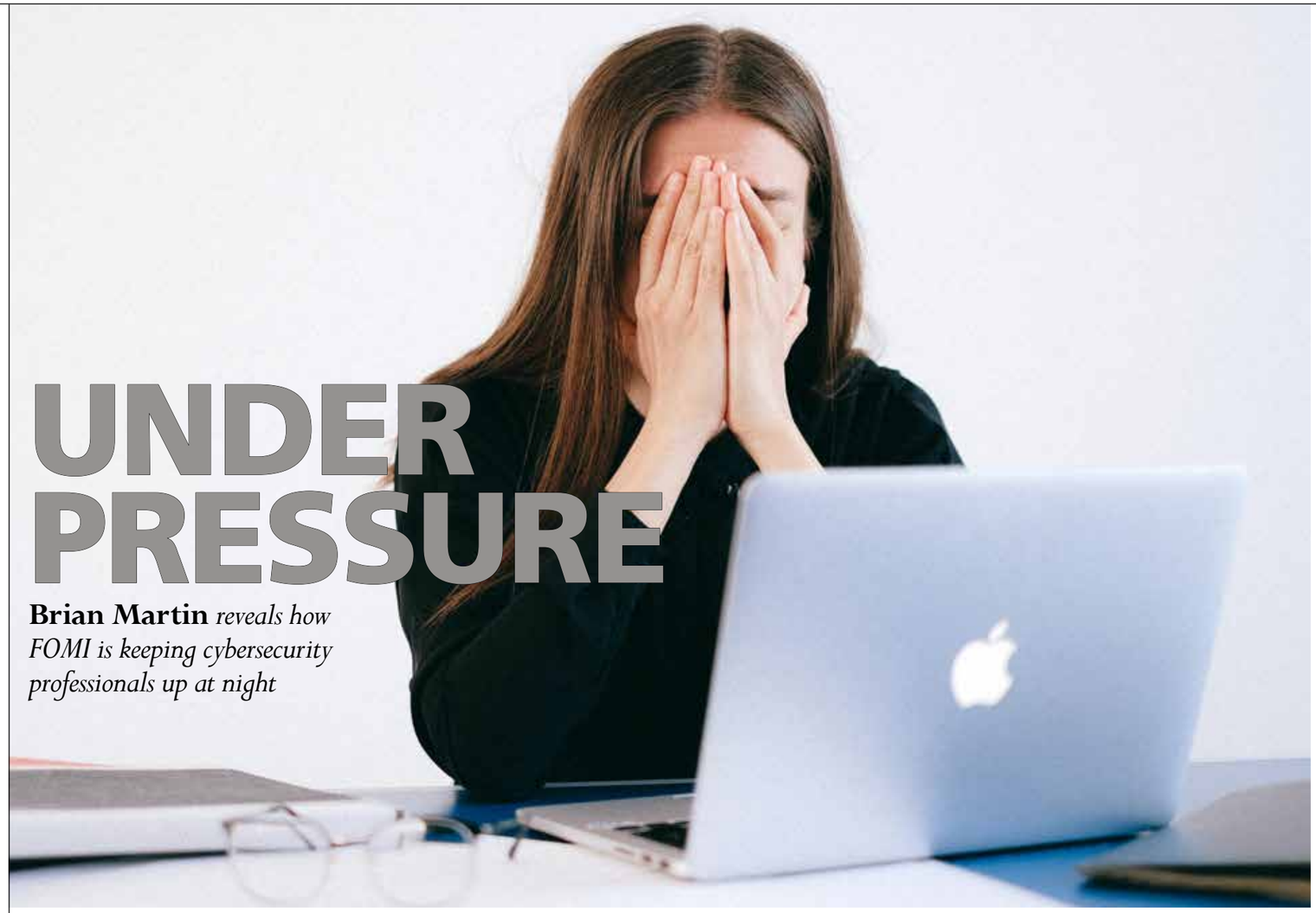

UNDER PRESSURE

Brian Martin *reveals how FOMI is keeping cybersecurity professionals up at night*

Most people have heard of FOMO (fear of missing out), but it's more likely to be FOMI – the fear of missing incidents – that's keeping cybersecurity professionals up at night. A small amount of pressure can sometimes be a good thing; if sustained correctly it can allow us to feel challenged, but not overwhelmed. Yet striking this balance is a delicate act.

Within the context of today's cybercrime arena, the tipping point for many security professionals was passed long ago. According to a report from FireEye, the average security operations team received over 11,000 security alerts every day in 2020, these volumes having left many industry professionals in situations where they are simply struggling to manage.

Such statistics, coupled with the fact that the average cost of a security breach is said to be $3.86-million, are telling of the pressures that analysts working in security operations centres (SOCs) are under. And it is easy to see why they are experiencing immense amounts of stress. Unable to overcome the rising tide of alerts, security experts continue to become more and more worried about pinpointing critical incidents that could lead to a series of adverse impacts such as data breaches, hefty fines and reputational damage.

A 2020 survey from Nominet quantifies this sentiment. The release, titled *The CISO Stress Report – Life Inside the Perimeter: One Year On*, revealed that as many as nine in 10 chief information security officers (CISOs) and chief security officer (CSOs) are experiencing either "moderate or tremendous" job-related stress. Further, 48 percent of the survey's respondents said that work-induced stress was having a detrimental impact on their mental health, with four in 10 stating that their relationships with their partners or children had been impacted.

It is worth noting that this survey was released in February 2020, prior to the first lockdown. Given the impact of the pandemic on the cyber arena, it is possible that these stress levels may have even risen in the year and a half since the report's release. Just two months later, in April 2020, for example, the FBI revealed that there had been a 300-400 percent increase in reported cybercrimes. And that upward trend has not reversed since, Check Point having reported that there had been a 102 percent increase in ransomware attacks during the first half of 2021 compared with the same period in 2020.

MDR helps to relieve the unwanted pressures of FOMI

This additional uptick in cybercrime is likely to have created a domino effect, leading to a further rise in alerts, and in turn added pressures to a FOMI pot that was already bubbling over. Placed under such strain, security professionals have been shown to be highly prone to burnout.

Despite being one of the most in-demand jobs of the modern day, often reflected by generous salaries, the average tenure for CISOs is little over two years. By comparison, a 2020 report from Korn Ferry reveals that the average tenure for any company executive is 4.9 years.

The problems presented by these mounting pressures are further highlighted by the International Data Corporation (IDC) in its recently released InfoBrief, showing the findings of a survey of 350 internal and management security service provider (MSSP) analysts and managers. Critically, it reveals that security analysts are becoming less productive owing to widespread "alert fatigue" that has led to a rise in ignored alerts, stress and FOMI.

The crux of the problem lies in the fact that almost half of all analysts' time is spent on false alerts, these comprising 53 percent of the total number of alerts received. Not only is this highly inefficient, drastically increasing workloads with redundant tasks, but it also creates significant risks for organisations – should alerts tick over an unmanageable number, security professionals may miss actual threats while responding to a false alarm. Unfortunately, this is the unavoidable reality facing CISOs, CSOs and other industry experts today.

The IDC's InfoBrief also states that 35 percent of in-house security managers admitted that they are simply forced to ignore certain alerts when their queue is maxed out. Given this context, it is easy to see why FOMI is a rising problem. The decision to miss certain alerts is taken out of nothing other than necessity, yet at the same time as many as three in four analysts are worried about missing incidents, with one in four worrying "a lot" and six percent losing sleep over it.

Security teams are doing what they can, but they simply don't have the resources to cover all bases. Indeed, the IDC affirms that only one in two CISOs feel they have the adequate tools to be proactive in their hunt for potential threats.

It is therefore clear that the pressure and stress placed on analysts is spiralling out of control in many instances. And with the volume and complexity of cyberattacks is only expected to rise over the coming months, it is a problem that – if not addressed – will only continue to get worse.

An answer is therefore needed. But the question is not simply about how these pressures can be alleviated. Rather, it is about how they can be alleviated in the most effective manner that benefits the individuals on the frontline while also providing a sustainable, scalable approach for the organisations that they serve.

On this front, many CISOs are turning to endpoint detection and response (EDR) and extended detection and response (XDR), both being emerging security technologies capable of delivering greater visibility, threat detection and response proficiencies across all corporate endpoints.

The former, EDR, powers the automated monitoring of endpoints, using behavioural analysis and machine learning technologies to instil advanced levels of protection far greater than that of legacy solutions such as antivirus software. The latter (XDR), meanwhile, is an even more evolved approach, taking the same principles of EDR and extending them beyond the endpoint to servers, networks the cloud, SIEM and other areas where vulnerabilities might be present.

Both EDR and XDR offer significant advantages, improving security capabilities and easing the burden on personnel. However, the key challenge with both approaches is that while automation may help to find risks, it can be hard to effectively respond to them without the right expertise. To truly transform security and address concerns surrounding missing incidents, organisations must take things a step further and tap into the skills of both humans and technologies through the deployment of managed detection response (MDR).

THE AVERAGE SECURITY TEAM RECEIVED OVER 11,000 SECURITY ALERTS EVERY DAY IN 2020

Defined by Gartner as: "*threat monitoring, detection, and lightweight response services to customers leveraging a combination of technologies deployed at the host and network layers*", MDR uses existing and emerging technologies like advanced analytics and threat intelligence in tandem with experts in incident investigation and response. It is this optimal combination of human and technology that helps organisations find (and deal with) potential incidents, vulnerabilities and threats.

The automated technologies underpinning MDR form its foundations. They can spot local threats and incidents that humans, because of the volume of alerts they are investigating, might miss. Given the current skills shortages facing the cybersecurity sector, this is vitally important. Estimations suggest that there are as many as 3.5 million unfilled cybersecurity jobs in 2021, with only one in four applicants for such positions ever actually being qualified for the roles they are looking to fill.

Meanwhile, another survey reveals that the vast majority of IT decision makers have a hard time finding and keeping experienced security staff and analysts to support workloads, while also experiencing difficulties in hiring, training, and keeping employees who can handle their organisation's full security tech stack.

MDR providers address this problem directly, offering trusted support that doesn't just flag potential incidents, but helps organisations respond to them as well, freeing internal enterprise security teams from alert fatigue. As we have already discussed, manually monitoring

and investigating alerts takes up an enormous amount of security professionals' time, with approximately half of all alerts being false alarms, and the result of this is stifled productivity, increased risks and weakened responses.

PLACED UNDER SUCH STRAIN, SECURITY PROFESSIONALS HAVE BEEN PRONE TO BURNOUT

Thanks to MDR, however, through the incorporation of modern SIEM technologies such as UEBA and SOAR, this challenge can be flipped on its head. When used in conjunction with a comprehensive suite of security tools, from intelligent incident timeline construction to automated response, modern SIEMs provide highly insightful context, showing how attackers think, their methods of work and their target assets. With these insights, security leadership becomes empowered, gaining the knowledge and tools they need to focus on delivering more effective results such as enhanced response times.

MDR is all about building up protection against an organisation's primary risks (be it data theft, hacktivism, compliance and others) while simultaneously supporting other priorities such as costs, productivity and the efficiency of operations. Every organisation is different. That is why a good MDR service provider will ensure its services are catered to the bespoke needs of the customer in question.

Such an approach goes far beyond off-the-shelf legacy solutions, mitigating the unique risks of an organisation based on its specific profile. Through bespoke security solutions, backed by the right combination of technology and security professionals, MDR helps to relieve the unwanted pressures of FOMI and enhance security in a multitude of ways.

It is a solution capable of identifying key risk mitigation requirements; offering detection and response on a 24/7 basis; employing detection and response use cases to mitigate risks; improving use cases to ensure they remain relevant; and building upon a company's existing tech stack across endpoints, networks, in the cloud and other risk areas. Given these advantages, the challenge of FOMI and the rising tide of security threats facing CISOs, now is the time for organisations to transform their SOCs ●

Brian Martin is Head of Product Management at Integrity360

While automation may help to find risks, it can be hard to effectively respond to them without the right expertise

Picture credit: Shutterstock