computing research

RESEARCH PAPER

No SIEM, no problem:

Why more technology and automation is not always the answer to all your cyber security headaches

December 2021

Sponsored by

FIELD EFFECT

CONTENTS

Introduction

As cyber threats and have become more sophisticated and more frequent, organisations have added ever more point solutions to their security stack – adding cost, complexity, and resourcing challenges. It's an environment that sees vendors thrive off upselling new solutions to customers as they seek to avoid featuring in the next data breach headline.

Businesses are now looking for new ways to combat this security infrastructure sprawl, often turning to SIEM solutions for centralisation of security events and greater use of automation and threat detection. While these routes have their benefits, they also come with their own problems and can be beyond the budgets of SMEs and smaller enterprises.

For all the technology advances, cyber security analysts continue to play a leading role in keeping organisations secure for the foreseeable future. And they can do this most effectively when supported by fully integrated, holistic approaches to security solutions – automating what is known, but relying on human analysts to keep customers truly secure and uninterrupted by alerts.

This white paper uses bespoke research findings to reveal how SMBs and small enterprises can overcome their alert fatigue, resourcing challenges, and security infrastructure sprawl, without blowing their budget on SIEM and bleeding-edge automation.

Computing surveyed 150 technical decision makers drawn from a wide cross-section of industry, including education, finance, manufacturing, government, and technology – with 90 per cent of organisations employing more than 500 people. More than 50 per cent of respondents were IT director level or above, and all respondents were directly involved in cyber security strategy or implementation.

Key findings

Organisations face a complex matrix of security challenges and an ever-growing threat landscape, set against tight budget constraints. Deciphering false alerts from genuine threats, and then triaging attacks, is a time consuming and resource intensive activity.

These issues are seeing some organisations adopt SIEM. However, for all its strengths, the real-world experience may not measure up to the sale pitch, particularly for smaller organisations. Instead, such businesses can bolster their cyber security defences through a combination of integrated solutions and external analysts. *Computing* research finds this to be a highly successful arrangement:

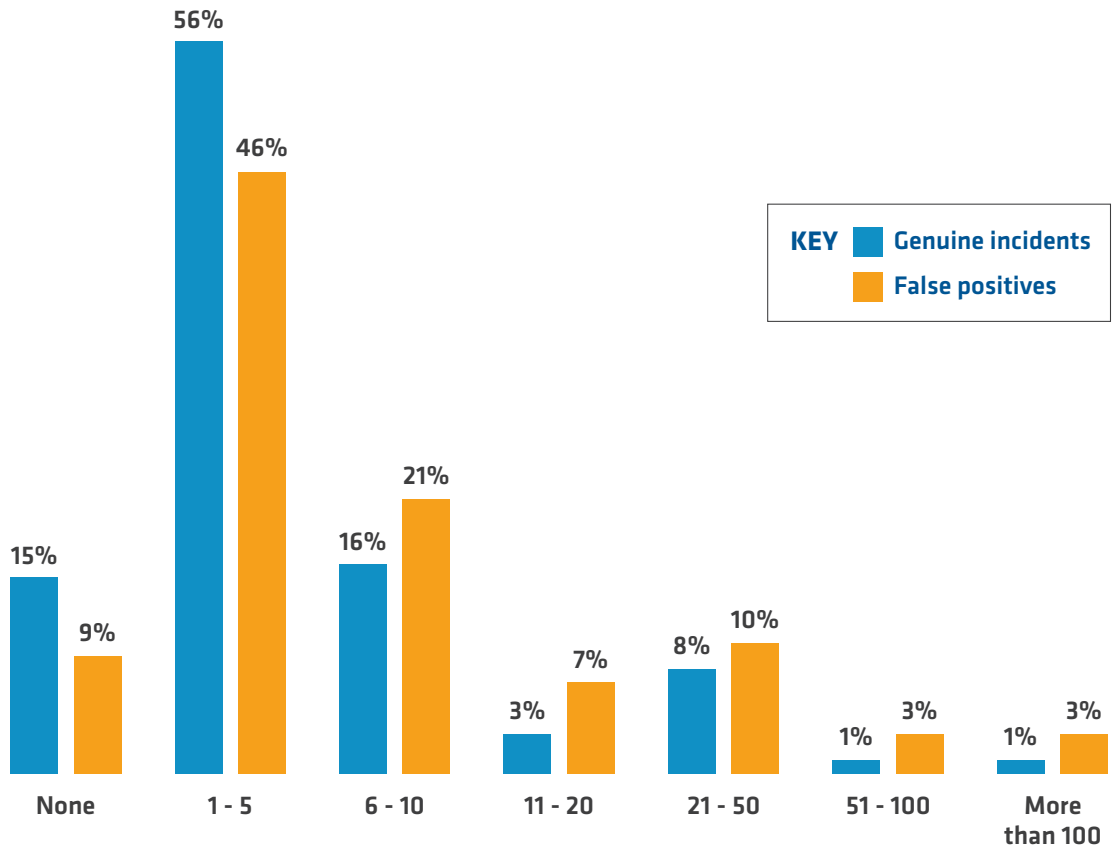
- SIEM solutions might address the challenge of finding a way to centralise and automate threat management, but this approach, particularly for SMBs, can be expensive and overlook the value of human analysis.

- The narrow application of a SIEM approach ignores where these systems become data and resource intensive, contributing to already overworked IT and security personnel workloads, as well as boosting already high false positive rates.
- Consolidated security solutions (rather than add-on point solutions that are upsold), combined with external security analysts, can provide a hybrid approach for smaller organisations that provides the security expertise and capabilities they require, without unrealistic budget and resource requirements.

A complex, challenging threat landscape

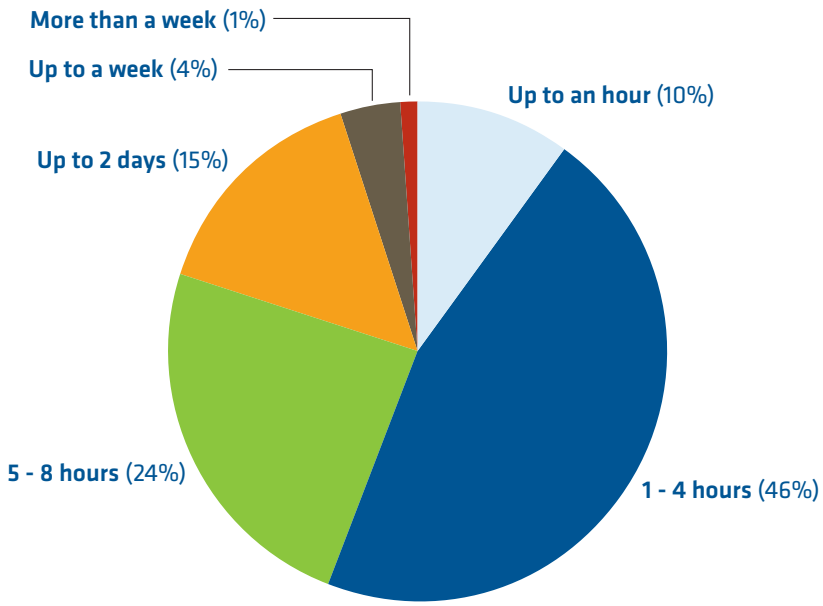
Organisations are dealing with a complex, fast moving and challenging threat landscape. Around 60 per cent of organisations have their security defences tested regularly, dealing with up to 10 incidents every week. These are genuine, potentially damaging attacks hitting them on a regular basis. At the other end of the scale, there is a small contingent of organisations recording no incidents or false positives. However, this seemingly clean sheet suggests these organisations may actually lack sufficient security visibility of their threat landscape.

Fig. 1 : How many genuine cyber security incidents and false positives do you experience per week?



What's even more worrying is that almost as many organisations are finding up to 10 false positive incidents in the same time period. This means a high percentage of organisations are having to manage and weed out a significant number of false positives from genuine incidents. When they are dealing with real-world incidents, it's a huge time sink, with almost 70 per cent spending between an hour to a full working day of eight hours, on average, working to resolve the incidents. Most organisations are spending many hours each week dealing with security incidents, and when you consider the frequency of genuine incidents, this is a massive resource demand.

Fig. 2 : How long does it take you, on average, to resolve a genuine cyber security incident?



Documenting the incident and maintaining an audit trail, along with distributing the incident report to the right people outside of cyber security in a timely manner, are equally the second-most challenges aspects of cyber security management. Just under 15 per cent struggle with reporting an incident, revealing a disturbing lack of support and inadequacies in a robust process that should more easily link identification to investigation and recovery.

When asked to identify the security challenges they're responding to and recording, phishing tops the list with more than half of survey respondents pointing to those socially engineering attacks, and malware/ransomware is an almost equal threat. Given that these can, in many instances, be delivered via email, it's surprising to learn organisations nominate email security as an area they're happy with in their securing defences.

Remote working and BYDO vulnerabilities figure prominently in their threat potential, a result of the rapid, wide-spread uptake of working from home driven by the pandemic. This is still leaving organisations vulnerable, as is a lack of security awareness and training. Drilling down closer reveals that more than one-quarter of organisations face security infrastructure sprawl and security alert fatigue, while 20 per cent simply do not have the adequate security infrastructure and tools.

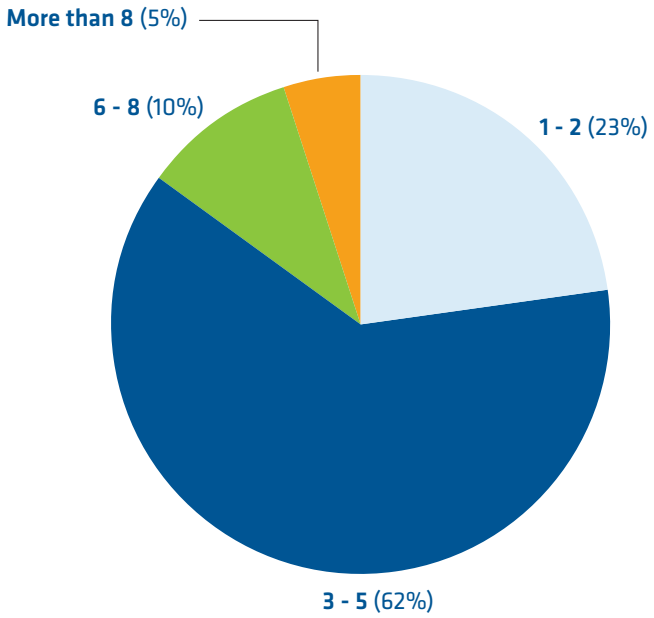
The combination of false positives, regularity of incidents, and time commitments goes a long way to explain why in organisations where there is limited human oversight, alert fatigue becomes a challenge. It's a real and present danger when incidents and false positive threaten to overwhelm the ability to decipher and respond appropriately.

SIEM Vs the alternatives

Cyber security solutions need to cover a whole host of workloads today, from email scanning and firewalls to cloud security and behavioural analytics. When looked at in its entirety, the security framework reveals itself as a complex patchwork of solutions, services and providers. This is born out in the research, which shows half of organisations are using up to five different security tools, and more than 40 per cent are have anywhere between six and 20 different active solutions. It explains why organisations, including SMBs, are juggling cost, complexity and resourcing challenges across their cyber security posture.

Figure 3 shows how many such tools must be accessed in the event of a security incident.

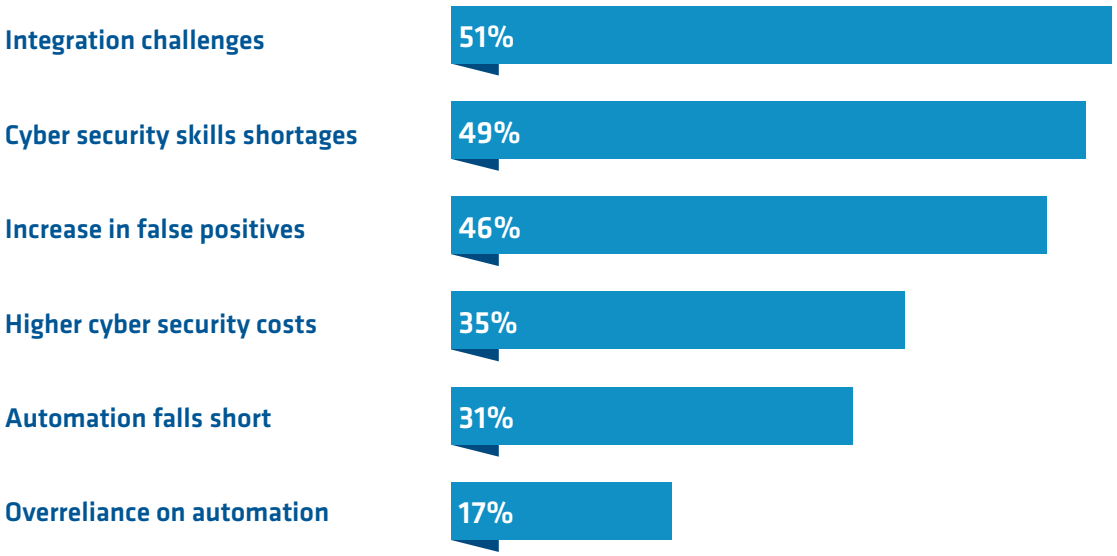
Fig. 3 : On average, how many security tools does one of your security analysts have to access to triage, investigate and remediate a security event?



The time-consuming and onerous remediation process that starts with deciphering false positives from genuine threats described in Figure 3 can be attributed to the multitude of disparate tools involved in the process. For instance, if there's an incident, 70 per cent of those surveyed will use between three and eight different security tools to triage, investigate and remedy. More broadly, when including the total number cyber security tools used in participating organisations, almost a third will use up to 10, while 15 per cent up to 20 and a number even more than this. It's an approach that is hugely costly, both in terms of the solutions themselves and the requirements to manage all of the different elements.

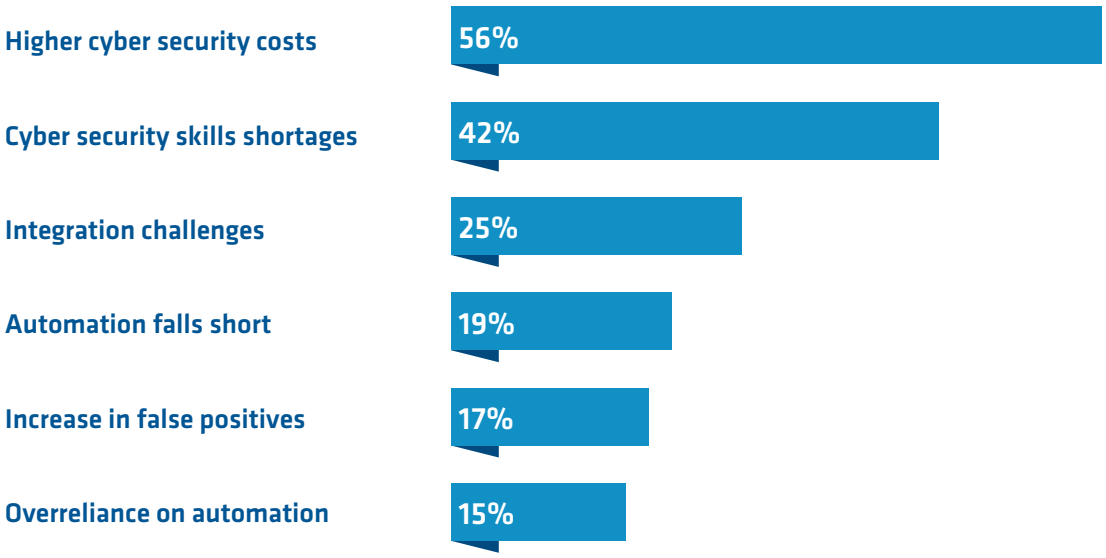
Looking to mitigate the drain on resources and attention from being buffeted by alerts and incidents, organisations may turn to security information and event management (SIEM) solutions. Whilst they promise to overcome some of the security technology sprawl challenges already outlined in this paper, it requires the successful integration of these tools. In practise, over half of those using SIEM have found this challenging and the experience has shown almost a third have had mixed results. In part, this is likely due to a lack of internal skills – cited by around half of respondents to the survey. The other challenges organisations going down this path face are increased costs and inadequate, or an overreliance on, automation.

Fig. 4 : Which of the following hurdles have you encountered through the implementation and running of SIEM solutions?



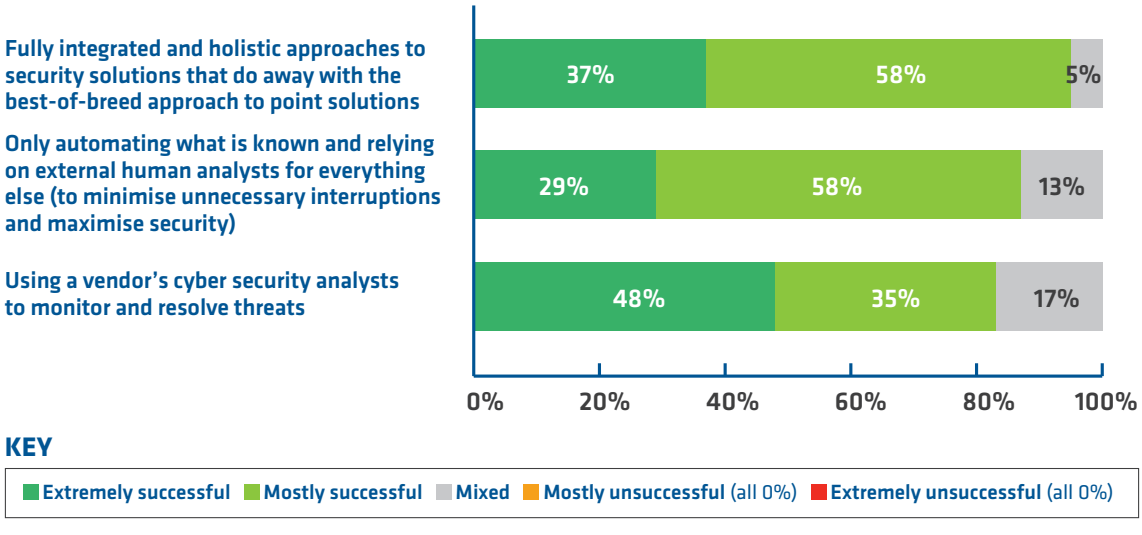
Those that hold SIEM adoption plans, cite higher cyber security costs as the most powerful deterrent, followed by a shortage of applicable cyber security skills and the technical challenges of integrating this with existing infrastructure. Looked at this way, it's clear how SIEM solves one problem but creates a batch of other issues – the last thing any organisation, large or small, needs when the priority must always be risk minimisation, cost control, and ROI.

Fig. 5 : Which of the following have deterred your organisation from implementing SIEM solutions?



Organisations that have opted for SIEM alternatives have seen widespread success, with a sizeable 95 per cent of those consolidating their security stack finding the initiative either extremely or mostly successful. It's a convincing vote of confidence and measure of success in real-world conditions. A slightly different take is to opt for selective automation – often relying on third-party analysts to minimise interruptions and internal resource demands, and compensate for internal skills shortages. This approach also saw broad success. Given the comprehensively positive experience, it's no surprise so discover that no respondents said these strategies had been mostly or extremely unsuccessful.

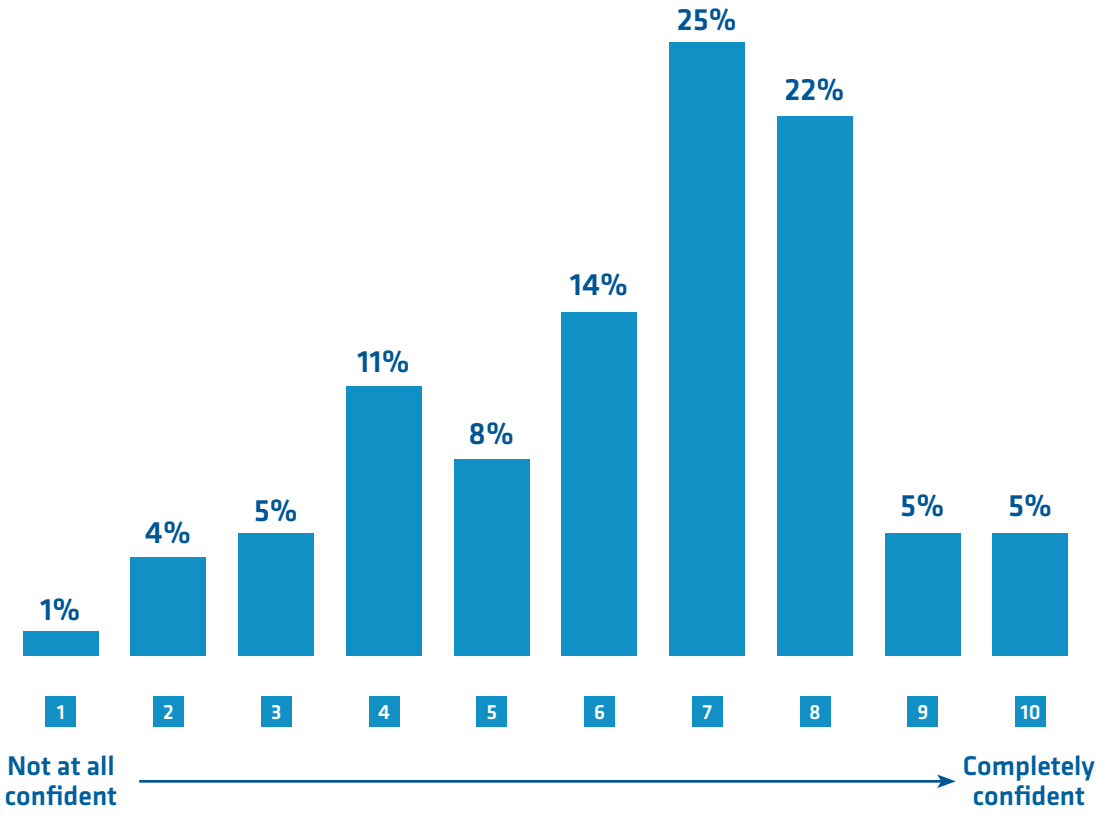
Fig. 6 : [Those that have implemented the following alternatives] How successful has your organisation's use of the following SIEM alternatives been overall?



The gap in security strategy

Organisations view their organisational security strategy as being sufficient in very limited applications, with only around half nominating their firewall and email security as areas they are completely happy with. Far fewer have faith in managing Zero Trust, vulnerability management and web security. And even when it comes to the security of critical business applications – an area that in itself would demand robust security – some three-quarters of respondents are not entirely confident in this security.

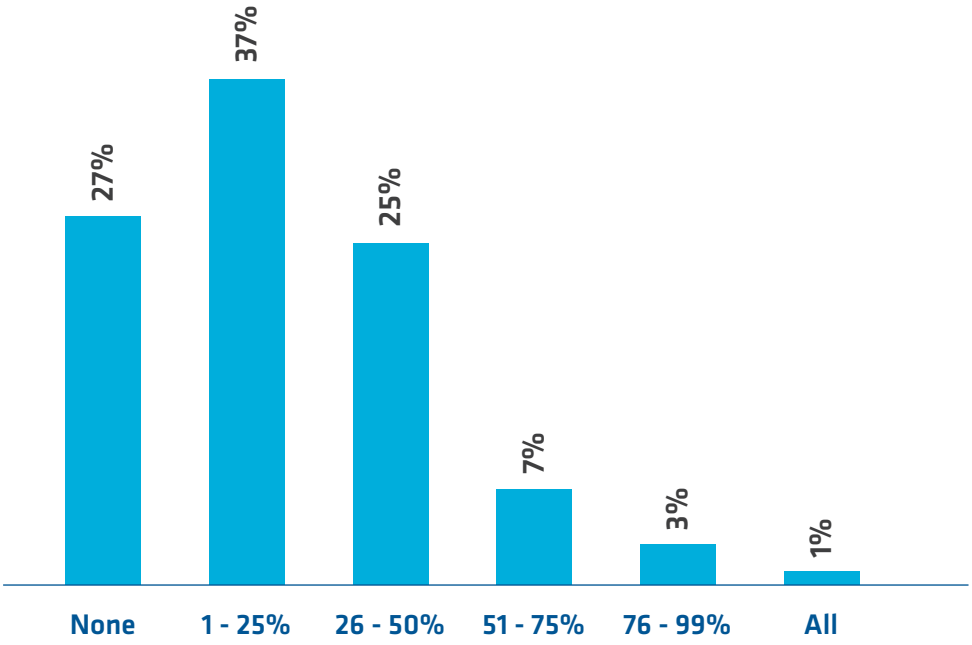
Fig. 7 : On a scale of 1 (not at all confident) to 10 (completely confident), how confident are you that your internal security resources have the skills required to effectively mitigate security threats?



Tellingly, although not surprisingly, few organisations have high confidence that their internal security set-up can effectively mitigate the threats they face week in, week out. Likewise, very few believe they have visibility of security threats and can prevent or contain threats. Given the volume of threat alerts and the task of sifting the genuine from the false flags, it's no wonder there's so little confidence in their organisation-wide comprehensive threat defence.

Some turn to external service providers to handle the complex security challenges. Looking at the degree of outsourcing in more detail, responses indicate that almost three-quarters of those surveyed are outsourcing to at least some degree. In particular, 62 per cent are outsourcing up to half of their security functions, while 11 per cent outsource over half.

Fig. 8 : What proportion of your cyber security functions are outsourced?



Looking ahead, over half of organisations expect to shift their security operations towards external providers over the next three years, primarily motivated by boosting their security capability. For others – a lack of internal expertise was a main motivation for 38 per cent, 39 per cent simply wanted a second pair of eyes to bolster their own security efforts. Some 32 per cent are looking for cost savings. For many smaller organisations it simply doesn't make financial sense to invest in internal SOC or SIEM capabilities.

Fig. 9 : How do you expect your use of external security providers to change in the next three years?

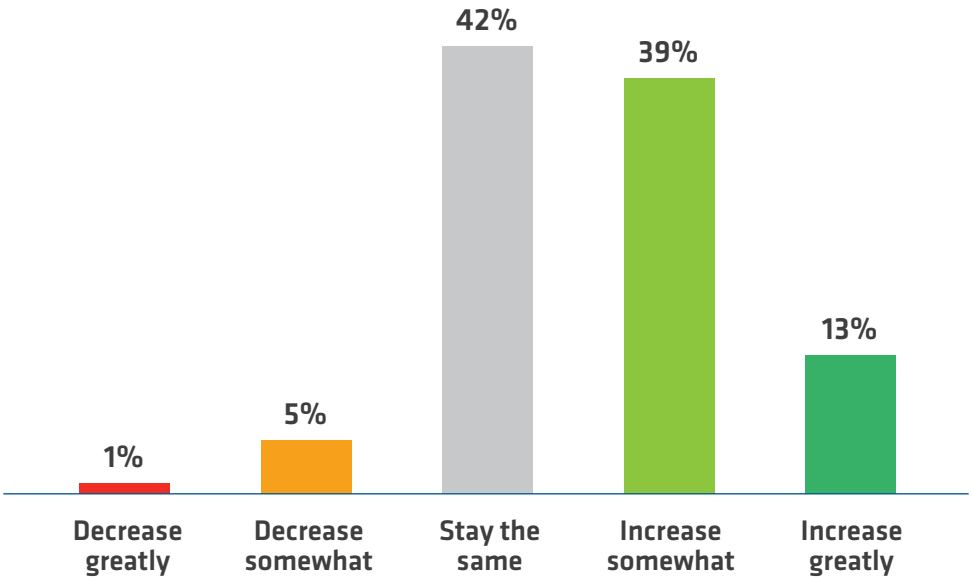
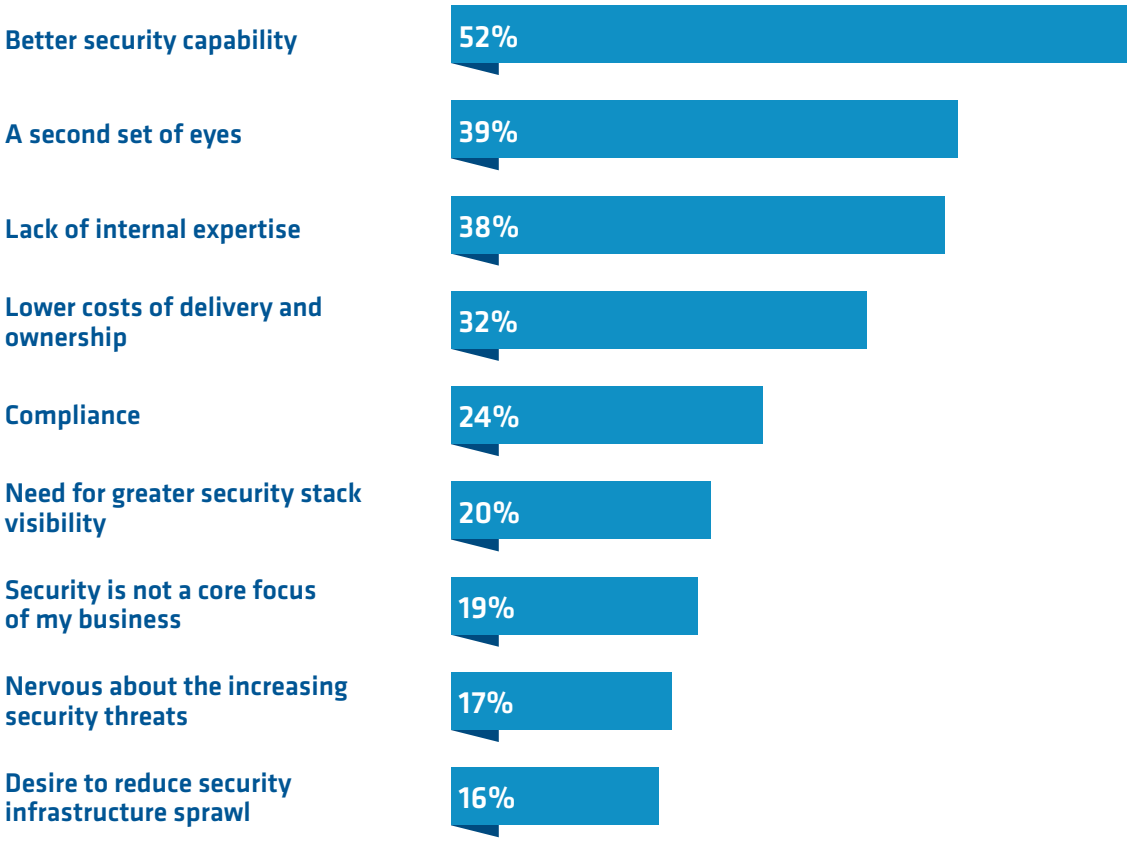


Fig. 10 : What are your main motivations for outsourcing your cyber security?



Conclusion

A complex matrix of security shortcomings and an ever-growing threat landscape, as well as constant budget constraints, could push some organisations to look for solutions like SIEM, believing it is the answer to their cyber security challenges. Yet, for the one-third of organisations currently running their operations through SIEM, they still face a range of hurdles in implementing and running these systems, starting with the challenges in integration. Once it's operational, almost half report they're seeing an increase in false positives and about the same facing a cyber security skills shortage.

It seems the reality of opting for a SIEM solution as the answer to the many cyber security challenges an organisation faces may not deliver in the end. While SIEM may prove beneficial to your organisation, it's important not to view it as a silver bullet solution.

It's evident that when it comes to managing cyber security, despite the plethora of solutions and the sales pitch about SIEM as the one-size-fits-all solution, organisations still find key cyber security tasks problematic. To minimise the impact, a security incident requires fast-moving remediation but, despite the very real urgency, almost half of survey respondents find the sum

total of this process challenging from the outset – starting with security incident identification, the follow-on process of investigating a breach and then making swift decisions to allocate the resources needed to deal with the incident.

This research paints a picture of SIEM solutions, while beneficial to some organisations, being simply not the right fit for others. Particularly smaller organisations that don't have the budget or expertise to make this approach a success. SIEM can quickly become too expensive for many, especially when considered within the context of a patchwork of point solutions that SIEM hopes to knit together.

Furthermore, these findings demonstrate the value of opting for consolidated security solutions, rather than add-on point solutions that are upsold, while drawing on external security analysts to fill in both the resource and expertise gaps that many organisations struggle with.

About the sponsor, Field Effect

Field Effect's award-winning Covalence® threat monitoring, detection, and response solution – powered by industry-leading technology and a team of cyber security experts – provides intelligence-grade cyber security protection for your network, cloud services and endpoints. Identify, prioritize, and remediate threats from one easy-to-use platform. Covalence provides its threat data as clear and actionable reporting that helps you understand your threats as Actions, Recommendations, and Observations (AROs). Our proprietary approach removes noise, showing you the alerts that matter with the context to resolve them. Designed to reduce cyber security complexity and costs, you gain a single source of protection to stop cyber attacks across your entire IT infrastructure.

For more information:

Visit: www.fieldeffect.com