SECURITY OPERATIONS CHALLENGES 2020

A Bytes Market Report

BYTES

Smarter
together

About this Market Report

Security Operations teams are facing the perfect storm with an unholy trinity of challenges to grapple with:

Cyber threats have never been greater. According to research by Forrester Consulting of 416 security and 425 business executives, just under half of organisations said they experienced at least one "business impacting cyber-attack" related to COVID-19 in April 2020, and more broadly, 94% of executives say their firms have experienced a business-impacting cyber-attack or compromise within the past 12 months.

Not only are attacks on the increase, but confidence in the ability to detect and prevent them is floundering. In a recent survey of 327 security professionals by the "Enterprise Strategic Group (ESG)" and the "International Systems Security Association (ISSA)", 68% of respondents said that cybersecurity technology and service vendors should be doing somewhat or a lot more to address cybersecurity challenges. Most respondents also said that the cybersecurity community at large, government agencies, and public schools should all be doing more.

Then there's the skill shortage and job disillusionment to consider. In the same survey by the ESG and ISA:

- 68% of respondents said they don't have a well-defined career path
- 65% said their companies don't provide enough training
- 45% believe the cybersecurity skills shortage has gotten worse over the past few years
- 29% said they've experienced significant personal issues due to job stress or they know someone who has

And finally, there is intense pressure on security budgets. In a survey published by McKinsey & Company in July 2020, more than 70 percent of security executives stated they believe that their budgets for fiscal year 2021 will shrink and for corporate security-operations centres, the cost needed to secure the fundamentals could reduce budgets for more advanced threat-intelligence upgrades, behavioural analytics, and other tooling.

To understand the impact of these challenges on UK Security Teams, we surveyed 190 UK IT Professionals ranging from IT Managers, CISOs, and Heads of IT from a variety of organisations.

This report provides their views and includes further insights and commentary from Luke Kiernan, Head of Security Alliances from Bytes Software Services, Sam Humphries, Security Strategist from Exabeam and Matthew Rhodes, Senior Channel Business Manager from Palo Alto Networks.

A Business Impacting Cyber Attack

"That is, one resulting in a loss of customer, employee or other confidential data; interruption of day-to-day operations; ransomware payout; financial loss or theft and/or theft of intellectual property."

Report Summary

What is clear from the findings detailed in this report is that Security Analysts are feeling the pressure and more needs to be done to put forward compelling business cases to justify the need for more investment into automation.

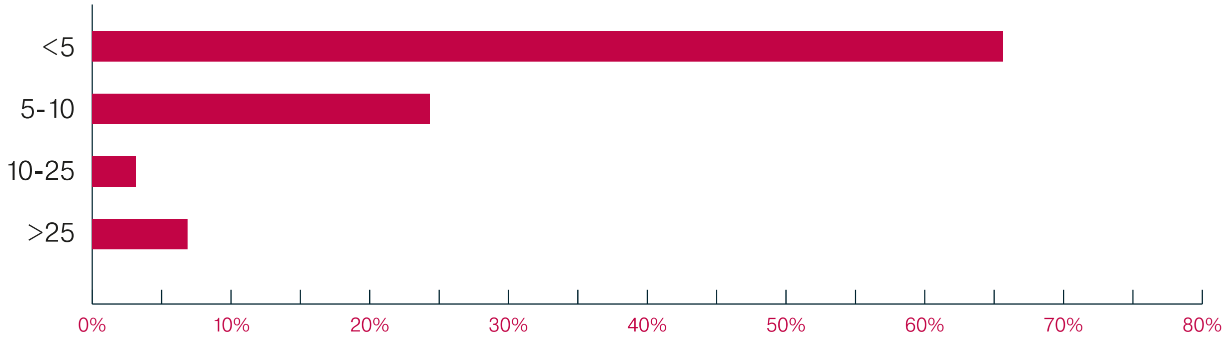
Solving the problem needs to be a joint effort between those on the front line and those running the organisations. Without such a coordinated approach, employee attrition rates will continue to rise and so too will security breaches.

The survey surfaced some interesting and alarming findings:

1. There is a material need for more budget and resources. As the threat landscape continues to evolve and solidify, 70% of respondents state they are under resourced and don't have the budget they need to counter the threats.
2. Attrition rates are at an all-time high. Finding good analysts is hard enough but keeping them motivated is proving even harder with 58% of respondents stating analysts typically stay in their job for less than 3 years. When the time it takes to onboard analysts is taken into consideration, this means most organisations are struggling to realise any material long term value from their security teams – putting the business at avoidable risk.
3. There is a severe lack of proactivity taking place. All the necessary proactive tasks, such as gathering threat intelligence, threat hunting and looking at ways to improve how the team operates are not getting the share of time needed to really make a difference. Far too much time is spent investigating known alerts and chasing false positives.
4. MTTD (ie, the time it takes to detect a threat) and MTTR (ie, the time it takes to respond to them) metrics matter, but too little attention is being placed on them. Indeed, of the respondents, 35% did not know their MTTD figure and 22% did not know their MTTR figure. That said, for the metrics to mean anything they need to be granular and related to types of threats or activities. The MTTD of a phishing attack will be very different to the MTTD of an APT. The same applies to MTTR. Time-based metrics are very important at a tier 1 / triage level, but once something is escalated then the quality of investigation is much more important. Operational metrics will drive behaviours, as ultimately you get what you measure, so should be reviewed on a regular basis. If the metrics look good but threats are still getting through then you're measuring the wrong things.
5. Confidence is low. Staggeringly, respondents were only 51% confident of detecting threats. This is the most alarming finding of this report and one we will look at a little later.
6. Automation is not a high enough priority. Almost 70% of respondents either don't have further automation on their roadmap within the next year, or not at all. Given the pressures being placed on the members of security teams, automation is an essential component of easing workload and improving confidence levels.

Despite the findings from this survey, there is light at the end of the tunnel as detailed later in this report.

How many people are responsible for security operations within your organisation?



While there is a correlation between an organisation's size and the number of security operations people they employ, there is an equally important correlation between the hours they need to provide proactive security management for and the size of the team needed to do it. When you consider Tier 1, 2 and 3 support – plus the necessary threat hunting resources and Team Leaders etc –without automated processes to alleviate the manual work, the minimum number of people needed to provide 24-hour cover is around 30.

Correlated to size, these findings show that most Security Operations Centres (SOC) are under resourced and under-automated for the service they are required to provide, thereby making it very challenging to provide the level of protection necessary in today's highly hostile cyber security landscape. As a result, threats are missed and organisations are exposed to unnecessary risk.

as a guide to best practice, taking Palo Alto Networks internal SOC as an example, for every 1,000 employees they employ they have one analyst in their SOC. This ratio is only possible and practical with a heavily automated environment where the investment they have made in automation means their analysts are able to undertake the more strategically important activities such as threat hunting.

Organisations with very small security operations teams typically find it hard to keep up with the workload and are forced to spend a high proportion of their time on more manual, repetitive tasks which often leads to employee disengagement and avoidable attrition. With a material skills shortage in the security marketplace, organisations can't afford to lose their analysts as replacing them is very challenging and a full time job.

This applies even more where SOC teams are small as losing one member of the team is set to have a higher impact on their capabilities than with a larger team. Automation for smaller teams to avoid staff attrition and enhance threat response capability therefore is arguably the best investment an organisation can make right now.

Simon Treen, Infrastructure Manager at The Clancy Group comments, "Don't underestimate the resource required to properly manage Security Operations."

What are the 3 main challenges that impact the efficiency of your security operation?

Pressure to do more with less resource/budget	70.9%
Not enough time or budget to automate mundane activities	43.9%
Too much time spent reacting and not enough time spent threat-hunting	40.7%
Too many manual investigations, so very labour heavy (and costly)	35.5%
Alert volumes are high	21.2%
Time spent chasing false positives	20.6%
Too much repetitive / mundane work	20.1%
Finding and attracting good talent	14.8%
Attrition of analysts	6.4%

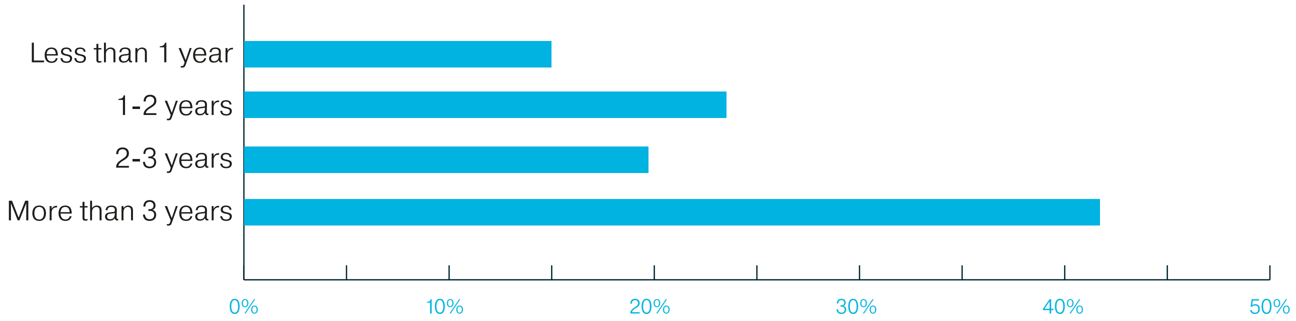
Perhaps the most alarming findings from this question are the high percentages of respondents that cited, "Too much time spent reacting and not enough time spent threat hunting" (40.7%) and "Too many manual investigations, so very labour heavy (and costly)" (35.5%). Combined, these statements highlight that analysts spend over 75% of time reacting and undertaking manual work, much of which could be automated. This not only increases the risk of threats getting through, but also has a direct impact on analyst attrition. There is light at the end of the tunnel however, as security intelligence tools can minimise the amount of time spent investigating threats and improve analyst morale.

The general findings from this question scream "automation". Time is clearly the most precious resource within SOC/Security Operations teams. The only way to ensure current team members can do more is to provide them with the tools they need to perform their tasks more efficiently – and technology is the answer. The challenge in many cases however, is that many organisations know they need to automate but they either don't know how to do it, or they haven't been able to convince the budget holders to release the right level of investment needed to do it.

Unfortunately, it's still the case that most SOCs don't get the funding they need until something goes wrong. One reason for this is the way the business case for investment is made as often they are not structured in a way that captures the imagination and urgency of the influencing committee. This is certainly an area Bytes can help with as we have a good track record of helping security teams achieve the funding they need.

Without sufficient resources, including investment in automation and training, analysts are often expected to do low-interest repetitive work that, over time, can lead to disillusionment and avoidable attrition.

How long do your Security Analysts typically stay in their role with you for?



The findings from this question are concerning, but unfortunately in line with expectations. While the "More than 3 years" has the largest percentage of respondents, it is masking a bigger concern, and that is that 58% of respondents stated that their SOC members leave within their first three years in the role. What's perhaps even more concerning is that over a third of respondents (38%) state that their SOC members leave in either less than a year, or 1-2 years.

Although training and on-boarding periods vary, assuming it takes 6 months to train up a typical SOC analyst, these findings show that 15% of organisations receive, at best, 6 months service from their newly hired analysts, and a further 22% only receive a year longer. When you consider analysts are in short supply, hiring someone that's trained can be a costly exercise, both from a hiring process and a salary perspective. Organisations therefore need them to stay employed for as long as possible. Even if less skilled analysts are hired, the hiring and on-boarding costs are also high so if people leave their role in their first 2-3 years there is a lot of associated wasted budget that could be better invested in making the SOC an interesting, efficient and enjoyable place to work.

The underlying question is, why are analysts leaving so soon? Is it the volume of mundane, manual tasks highlighted in the previous question? The findings from the next question will help provide some insight to this.

It is important to note that if automation is used correctly, tackling the repetitive events analysts spend most of their time on, it is likely that they would remain in-role for longer. In theory, they would apply more time to a smaller number of novel and mentally testing tasks, allowing for enhanced development and enrichment.

After all, staff turnover is both resource draining and damaging to team moral. Preventing it, and creating an engaged, driven team should be a priority.

What % of time do your Security Analysts typically spend:

	<10%	11-25%	26-50%	51-75%	>75%
Triaging level 1 alerts	43.09%	29.26%	19.68%	7.98%	0%
Investigating level 2/3 alerts	30.43%	33.70%	31.52%	4.35%	0%
Chasing false positives	43.48%	30.98%	16.85%	6.52%	2.17%
Gathering threat intelligence	45.90%	36.61%	12.02%	4.92%	0.55%
Proactively threat hunting	68.54%	17.65%	6.95%	5.88%	1.07%
Improving the way the team operates	60.54%	22.70%	12.97%	3.24%	0.54%

The findings from this question are insightful, alarming and useful when trying to understand the attrition trend previously mentioned.

Let's start with potentially the most alarming finding, and that's to do with the time spent "Proactively threat hunting". Arguably one of the most important SOC activities, and yet 86% of respondents state less than 25% of time is spent doing this - and even more concerning is that over 68% of respondents state less than 10% of time is spent doing this. Not only is this activity essential in combatting security threats, but it is also very interesting work and something analysts like doing.

The more they are exposed to such activities, the longer they tend to stay in their role, thereby helping to keep attrition levels under control.

Considering the above, what's also concerning is the amount of time that is being spent gathering threat intelligence. 95% of respondents state that up to 50% of time is being spent doing so, and yet, only a fraction of time is being spent proactively threat hunting – it begs the question, why invest time gathering intelligence if you are not going to make the time to investigate the discoveries.

Another alarming finding here is the amount of time being spent "Improving the way the team operates".

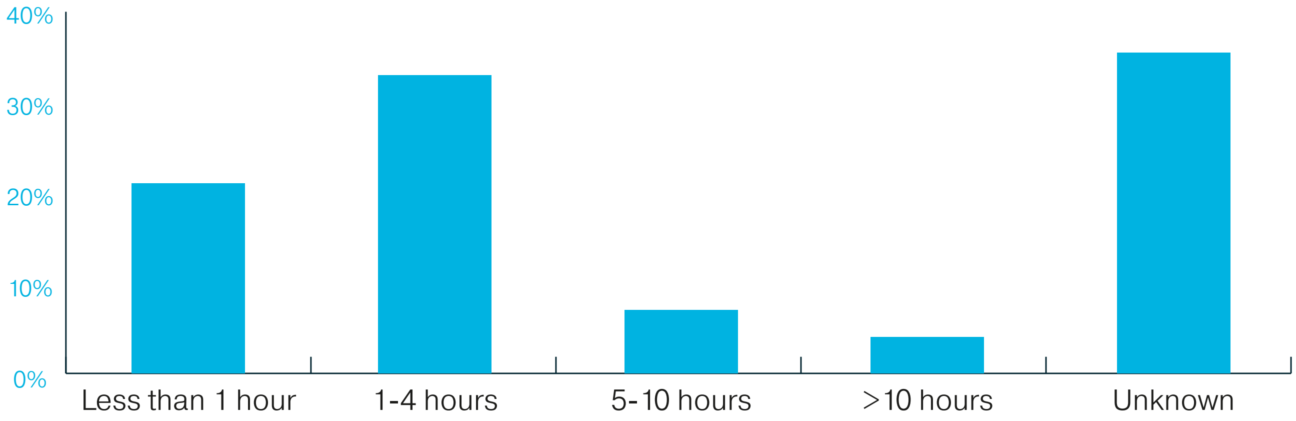
60% of respondents state less than 10% of time is being spent doing this, and 83% state less than 25% of time is being spent doing this. If improvements are not made to how teams operate it presents no opportunity for efficiency, innovations, work variety or staff development. This can result in tasks becoming mundane, employee disengagement and dissatisfaction, avoidable attrition, avoidable re-hiring and onboarding costs.

Another point of interest from this question's findings is the amount of time analysts are spending investigating level 2/3 alerts.

Over 95% of respondents state that up to 50% of time is spent doing this. When you consider that an alert relates to a known threat, this is a material amount of time to spend on this activity, particularly given the lack of time spent investigating unknown threats.

James Fleming, CIO at Element Materials Technology, comments, "Automate what you can and remove as much mundane work as possible. It helps to keep talent and can also improve detection rates."

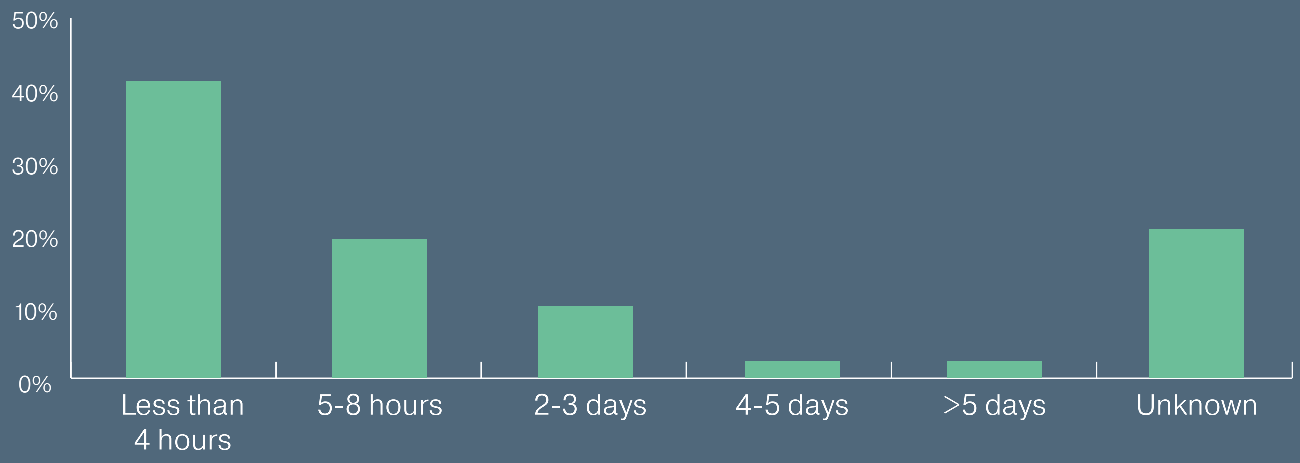
How long does it typically take you to detect threats (MTTD)?



The point of note in relation to these findings is the "unknown" category. 35% of respondents do not know how long it typically takes to detect threats (MTTD). This suggests almost a third of organisations do not have the required management metrics and/or the processes and technologies in place to monitor the performance of their SOC.

Without focusing on metrics such as the MTTD, improvements to the SOC will be hard to a) identify, and b) justify. The findings from this question will be directly impacting the "What are the 3 main challenges that impact the efficiency of your security operation" question covered earlier.

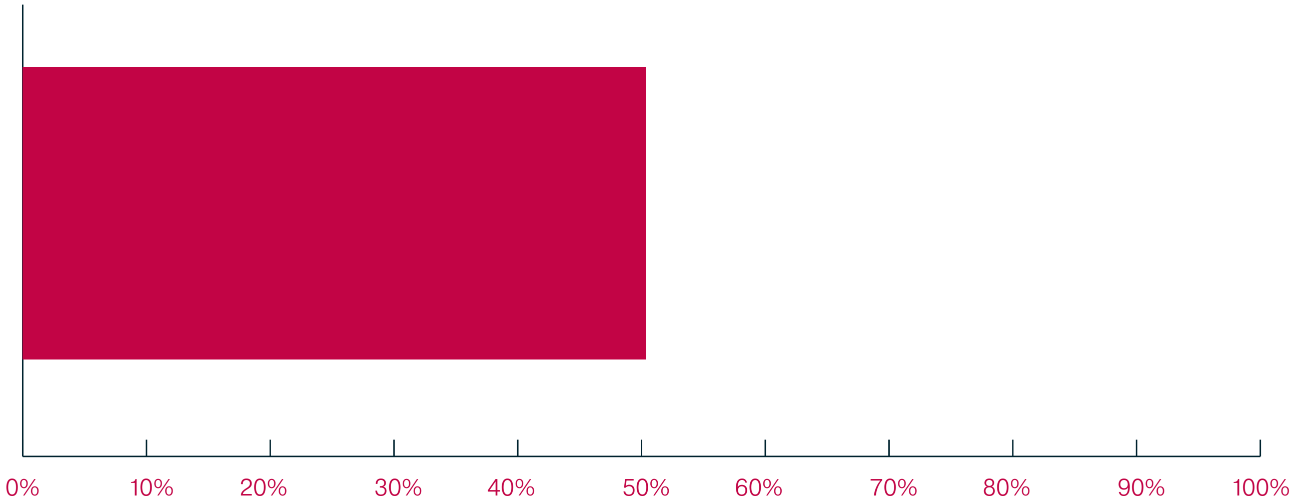
How long does it typically take you to respond to threats (MTTR)?



When looking to make sense of this question, the devil is in the detail as we need to understand the types of threats being responded to. That said, over a third of respondents stated they are taking more than 5 hours to respond to threats. When you consider these are known threats, this is far too long and suggests a lack of automation, due process and/or under resourcing of analysts.

The one finding that stands out is the 22% of respondents who state they don't know how long it is taking to respond to threats. Once again, this presents a major challenge when looking to secure funding to improve the status quo as without a clear metric to base the business case on, it will be virtually impossible to secure support for any budget or resource requests.

How confident are you at detecting threats?

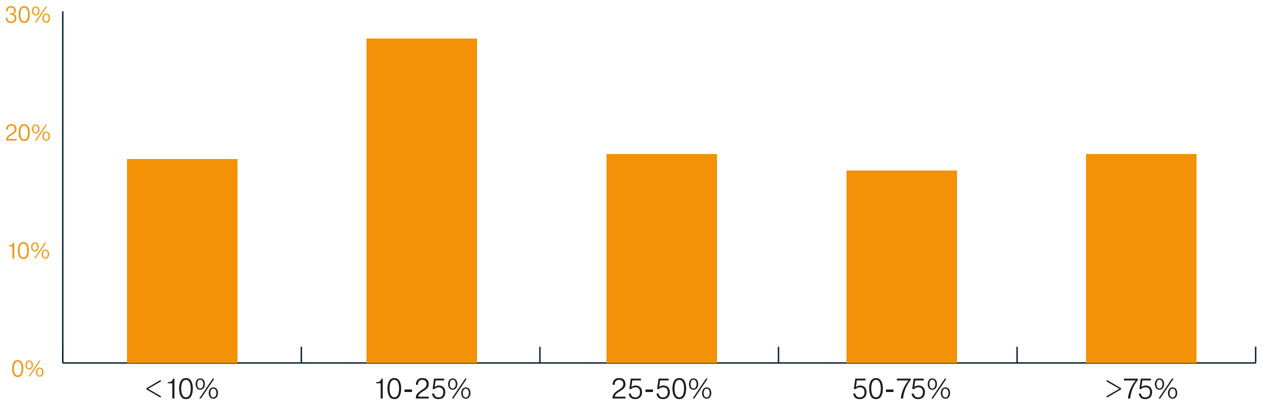


This should be the headline finding from this survey. On average respondents are only 51% confident at detecting threats. Let's come back to this in a moment.

In our previous survey, "Security Challenges 2020 – A Bytes Market Report" we asked a couple of similar questions. One was "From a people perspective, how confident are you that you are protected from such cyber threats" and the other was the same question but from a technology perspective. The respondents in that survey answered 71% and 78% respectively, so on average they were 71% and 78% confident in their people and technology.

While this question is more specific, the findings are vastly different from our previous survey and highlight a very concerning situation. If the reality is per our survey findings, action needs to be taken urgently to identify the reasons why people are only 51% confident in their ability to detect threats and the remedial action that needs to be taken. If budget/resources are needed to move the dial in the right direction, ideally with a target confidence score being 85%, the business case needs to reflect this. Once again, Bytes can help with as we have a good track record of helping security teams achieve the funding they need.

What % of alerts are being handled in relation to those being detected?

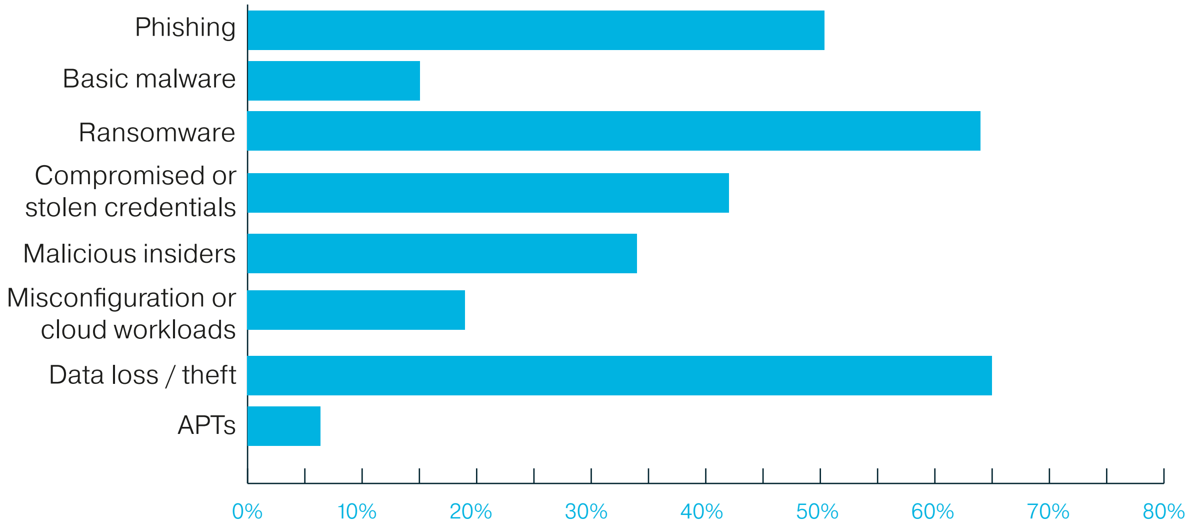


Two thirds of respondents are handling less than 50% of detected alerts – and remember, these are known “detected” alerts – how about those that are undetected? This again is an astonishing finding and underpins the “time is the most precious commodity in SOCs” statement made earlier. Organisations simply don’t have the right balance of people, technology and automation to effectively deal with threats in a timely manner in 2020.

Given everything we have so far discovered in this survey, the findings from this question are not that surprising as they are consistent with the lack of time/budget narrative.

Insights like this are useful to quote when building up the business case for more investment and feed into the “% Confident” question earlier.

What 3 threats are you most concerned about missing?



Some of the options given in this questions are the "means to the end", such as "Phishing", "Basic malware", "Malicious insiders" and "Misconfiguration of cloud workloads", while others are "the end", such as Data Loss and Theft and Compromises and Stolen Credentials.

While organisations may be concerned about missing Phishing threats and Basic malware, these threats have been around for many many years. Moreover, there are some very sophisticated and effective technologies on the market to prevent them, so with the right tooling, organisations should not be too concerned about these. The fact that so many are concerned about missing these threats shows the lack of maturity and threat detection capabilities of many SOCs at present.

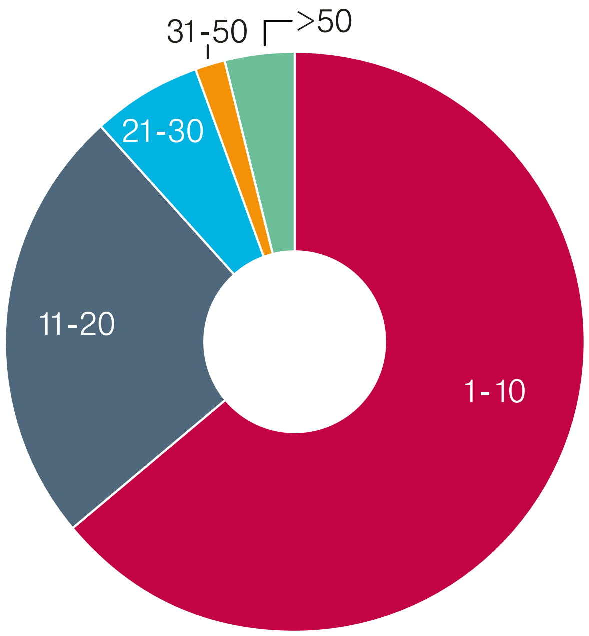
We are also surprised that only 18% of respondents listed Misconfiguration of cloud workloads as a concern at the same time as Gartner have published research stating that "through 2022, at least 95% of cloud security failures will be the consumer's fault," and that "through 2023, 99% of firewall breaches will be caused by firewall misconfiguration, not firewall flaws."

The number of respondents stating they are concerned about "Compromised or stolen credentials" (42%) is also too low. If credential compromise is not prioritised and acted upon the organisation will be being opened up to an avoidable breach.

Organisations are reporting concern around the ends of the attack chain, but aren't paying enough attention to the middle – such as what happens when an attacker gets into the network, or if they start out within the network (insider threats). Detecting these activities, such as the use of compromised credentials, can make the difference between a minor incident and a full blown breach.

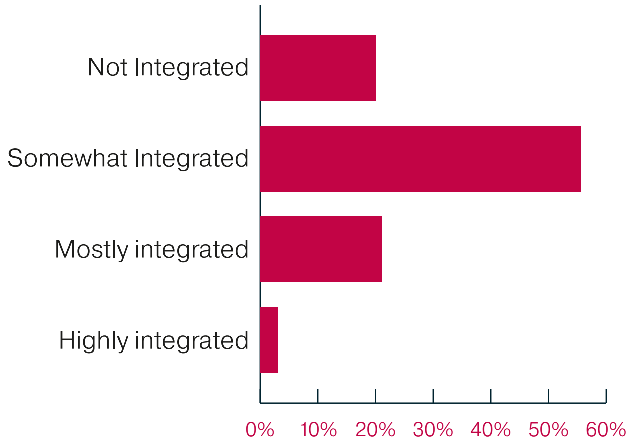
Exabeam's Advanced Analytics provides powerful user-behaviour detection capabilities to enhance an existing SIEM, or as part of a full Exabeam Security Management platform deployment.

How many technologies are in your security stack?



These findings are in line with expectations, however the next question is perhaps more interesting to analyse.

How integrated are the technologies?



Over 1/3 of respondent used 11+ technologies and dashboards in their security stack. Of those at the highest ends of the spectrum (using 21+ technologies) - just 13% of them classed those technologies as being highly integrated. What's more, nearly 80% of all respondents stated that their security technologies were only somewhat or not at all integrated.

This lack of integration, particularly where there are a lot of technologies in play, puts a huge manual burden on the Security Analysts to do their job effectively. Constantly switching from system to system is not only mundane and time consuming, but also will be exposing the organisation to risk as errors will undoubtedly occur. This will, without question, be the reason behind some of the inefficiencies already referenced in this report.

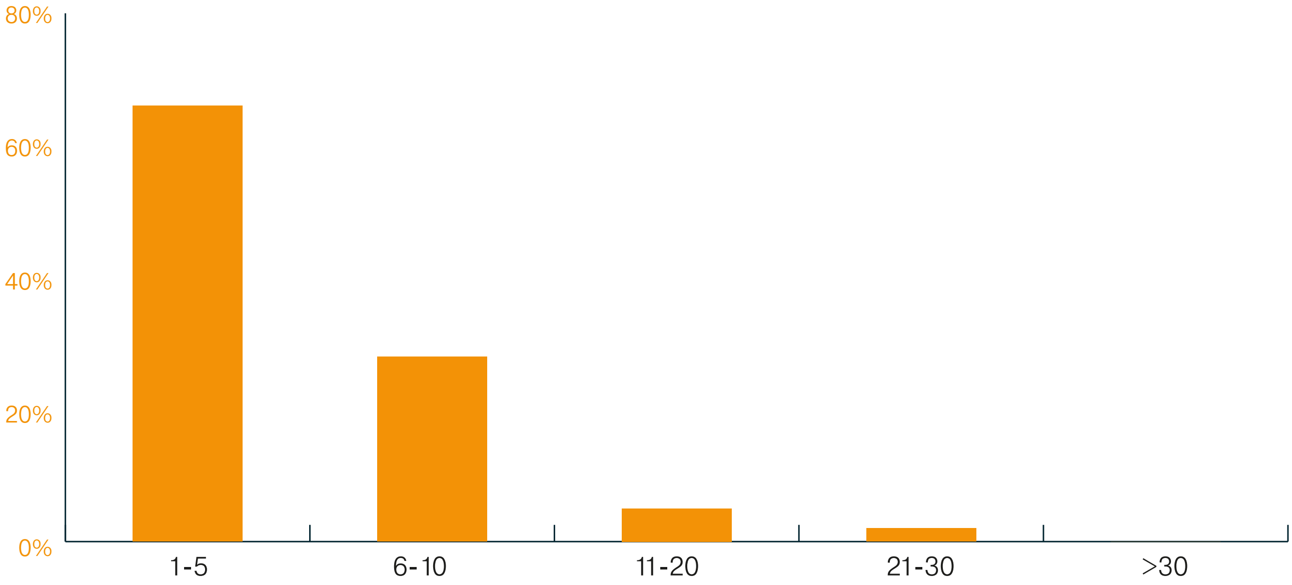
Too much time spent system-surfing is also resulting in insufficient time being spent proactively threat hunting.

Clearly not every technology can be integrated with another, but core systems should be and can be with the likes of Exabeam's next-generation Security Management Platform offering that has hundreds of out of the box integrations included.

Using such a solution, data analysis from across the security and technology stack can be easily enabled, helping to automate investigations and save analysts considerable time and effort.

Dan Shuttleworth, Associate – IT, Cyber Security at BDP, comments, "Integrate systems where possible, educate staff & management often and prioritise the area's most important to your organisation."

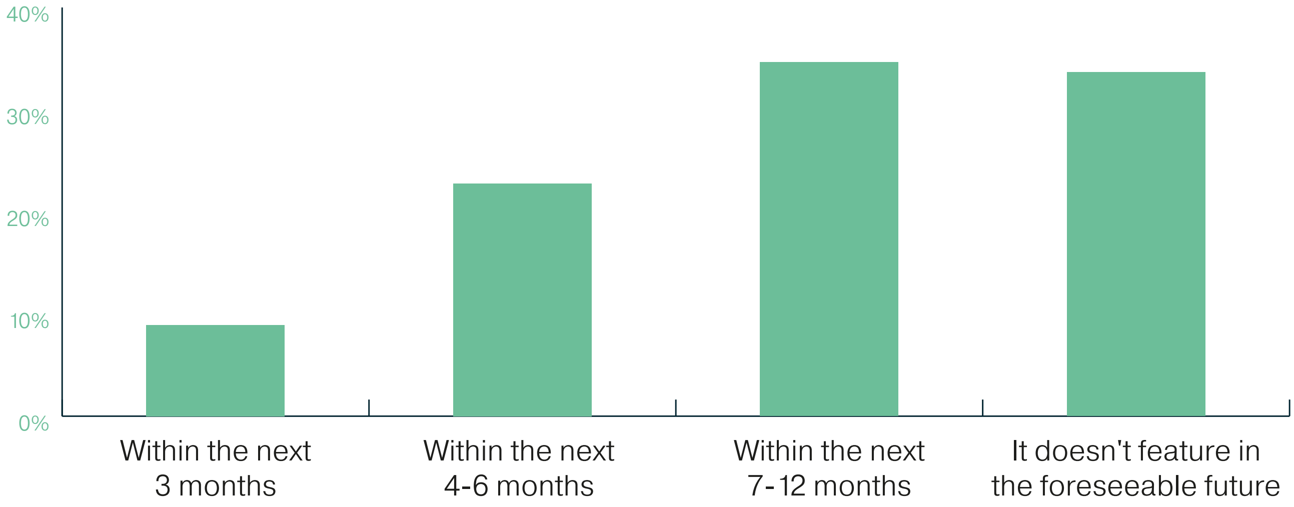
How many different tools do your security analysts use on a daily basis?



The fact so many respondents (>65%) stated they are using less than 5 tools daily underpins the lack of proactivity taking place in most organisations. Without automation or integration (which is evidenced in the majority of answers in this survey), to be an effective threat hunter necessitates mulitple tools. This lack of tooling and/or integration is therefore exposing UK organisations to significant risk.

Iain Jones, Infrastructure & Cloud Technical Consultant at Northumbrian Water, comments, “Tooling is fundamental. Does it address all workloads, is it integrated and can it filter the irrelevant information.”

How soon do you expect further automation to feature in your security operations roadmap?



Given the narrative in this report, particularly around the pressure on time and resources, amplified by the lack of proactive threat hunting taking place, there has never been a better (or more important) time than now to consider further automation.

The evidence shows that organisations everywhere are struggling to respond to known threats and proactively hunt out new ones. They are losing key team members and are only 51% confident in their ability to detect threats.

Given this, it is alarming that over a third of all respondents have no plans for further automation. Our experts put this down to a lack of understanding of what automation can deliver, particularly within the C-Suite.

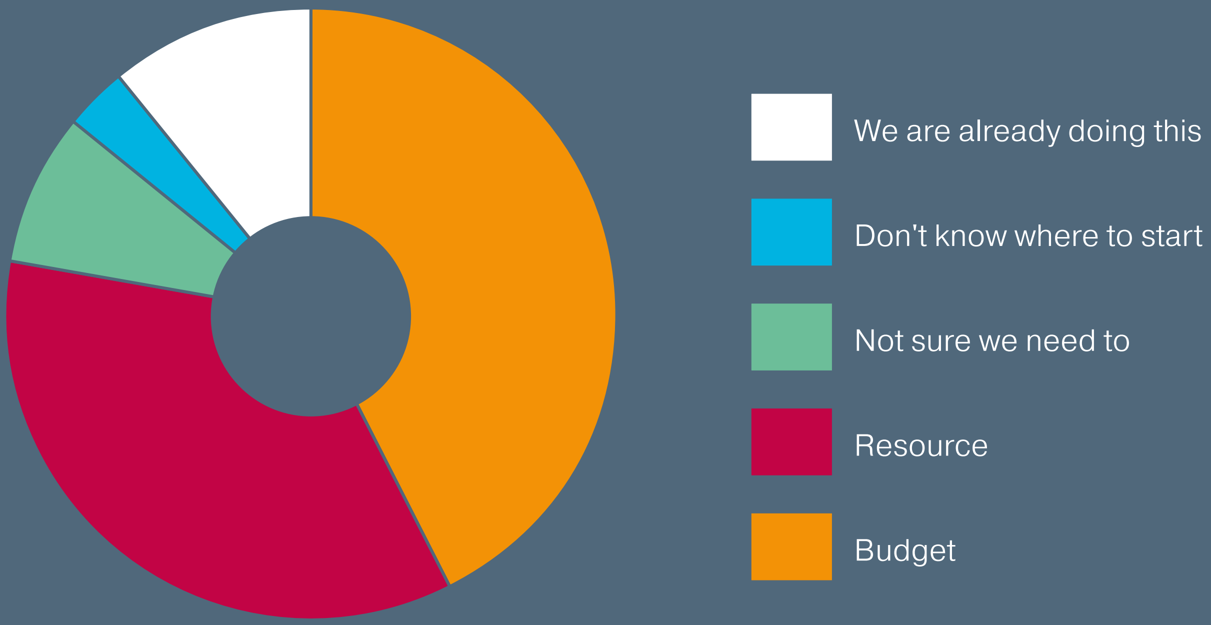
Organisations really are advised to research the cost-benefit automation offers and consider the impact of continuing without it.

As has been referenced several times in this report, Bytes has the experience and expertise necessary to help co-build a solid business case and are open to discuss our approach with anyone reading this report.

Automation saves money and frees up resources to focus on more important threat-hunting activities, thus delivering higher analyst satisfaction and vitally, levels of effective threat protection.

Ahren Stevens-Taylor, Head of IT Security and Networks at Packt Publishing agrees, “Automate as much as possible, and invest heavily in an extensible SOAR platform, it will reduce both the manual efforts of analysis and allow you to spend more time performing threat and vulnerability hunting (where the fun is).”

What is stopping you automating more of your security operations in the very near future?



If approached correctly, automation has many benefits, such as time and motion savings, enhanced threat-prevention and improved attrition. The first stage to developing an automation strategy is to identify and analyse your security operations posture. The findings of this review can then form the basis of a compelling business case that recommends investment into technologies and automation tools that will help ensure skilled analysts are better supported and able to defend against threats.

Bytes can help identify the areas that would most benefit from automation and can also contribute to the business case. More on this to follow later in the report.

Key Takeaways

The findings and narrative detailed in this report can be summarised as follows:

Time is the most precious resource within Security Operations and there is not enough of it to go around. Consequently, analysts are having to spend a disproportionate amount of their time chasing false positives and investigating level 2/3 alerts, instead of focusing their attention proactively hunting for unknown threats and looking at ways to improve the overall running of their department.

1. Analysts are generally unhappy in their role and are leaving organisations within 3 years. Much of this dissatisfaction is to do with the above and the repetitive, mundane and manual nature of their work, coupled with the stresses being placed on them. No-one goes to work to do a bad job but when the expectations of the job are too high disillusionment soon sets which can quickly impact the quality of the work being done.
2. Given the pressures being put on security teams and the lack of tools to help ease the pressure, there is an acknowledgment that threats are not being sufficiently quashed and an acceptance that many are probably getting through. This is reflected in the 51% confidence score stated earlier. It is not therefore that people have their head in the sand when it comes to the seriousness of the situation, quite the opposite, but more that people simply don't know how they can improve matters given the budget, tools and resources they have to work with.
3. There is a severe lack of fit-for-purpose tools being deployed within security teams. Going by the responses to this survey this appears not just to be a budget issue, but more to do with a lack of awareness of the benefits to be gained from investing in automation and enhanced SOC technology as well as a lack of energy into making the case that more investment is needed. While many organisations are looking to save money at the moment, most see the necessity in protecting their data so if company Directors were furnished with the facts in a way they could understand, many would make available additional resources and/or offer alternative solutions to help address the problems detailed in this report.

There is light at the end of the tunnel.

Defining the project brief and building a business case for more investment in security automation tools can be challenging. Fortunately this is what Bytes do day in day out. We have a solid track record of helping security teams secure the investment they need.

Automation can help:

- Reduce staff attrition as analysts have more time to use their skills and experience on the tasks and activities that matter most, and that are therefore most rewarding.
- Save time as many mundane tasks can be fully automated, alleviating the pressure on highly overworked teams.
- Improve processes and workflows so they are more efficient and able to speed up investigations.

Solutions such as Cortex by Palo Alto Networks and the Security Management Platform from Exabeam, who Bytes are a Platinum partner of, provide organisations with an ideal opportunity to fast-track their journey to automation by giving them the technology they need to help their skilled analysts do the job they are needed to do – protect the business from threats.

Future Trends

1

Avoiding the misconfiguration hazard.

As organisations accelerate their use of cloud platforms and applications to support the remote workforce, many will experience data breaches, due mainly to misconfigurations and lack of visibility into cloud applications, services and infrastructure. It is vital therefore that security and IT teams retrospectively apply due diligence to ensure gaps are closed and best practices followed.

2

Strength through diversity.

The upside of the proven new distributed working world will be a positive impact on the security skills gap, and diversity and inclusion in the industry. Security professionals, and in particular women, who have previously left roles due to family or other life commitments which meant they could not attend a 9-5 office environment now have access to WFH roles. Additionally, distributed working also opens availability of candidates in alternative locations, even other countries.

3

The next generation.

The importance of cloud security skills and secure coding practices will continue to grow at break-neck speed. People thinking of joining the security industry, either from higher education or cross training from other technical roles, should be looking to these areas of learning.

Dedicated Help to ensure Continuous SOC Improvement

“Automation applied to an inefficient operation will magnify the inefficiency.” - Bill Gates

Automation isn’t a silver bullet, and it won’t fix your broken processes for you. Automation does as you tell it. If you tell it to complete a broken or faulty process, it will. As a result, you’ll get broken, faulty results. They’ll be on a much larger scale, as automation efficiently replicates your inefficient operations.

Our survey findings showed that for many organisations, the current time and resource spent on optimising and reviewing their SOC processes and operations, is alarmingly low, with the vast majority surveyed spending less than 10% of their time looking for ways to optimise and improve.

Small wonder that so few are able to harness the considerable cost, time and threat detection enhancements available from automation.

If you are a business caught in this vicious cycle of being trapped reacting and not having the time, resources or skills to look seriously at improving processes and then breaking free with automation and SOC enrichment, consider speaking to Bytes about our free of charge Security Operations Strategy Review.

Get expert, independent advice on ways that your SOC can move forward with process, people and technology – so you can see the wood from the trees and:

1. Analyse your current and desire SOC performance
2. Identify immediate and long term improvement actions
3. Gain visibility of the business benefits from automation and enhanced technology
4. Build a roadmap to a more proactive operations team
5. Scope that roadmap into an actionable improvement plan.

Bytes dedicated security specialists can help you chart a smooth course through the often complex, murky waters of automation so you not only have clarity on what improvements you could make, but complete visibility of the impact of making those so you can be confident in the long term of outcome and business benefit from implementation.

As time is the most precious commodity Bytes, working with our partner ecosystem, can also provide full technical support on delivery should you wish to go ahead, so you can significantly reduce the time, cost and resources needed to implement improvements and/or automation in your SOC.

Getting expert independent advice on SOC process, people and technology improvements will enable you to remove the unessential, automate where appropriate and make your defences stronger and more agile against all forms of attack.

“It is not a daily increase, but a daily decrease. Hack away at the unessential. The closer to the source, the less wastage there is.” - Bruce Lee

Our quality process

Step 1: **Assess**

- Evaluate current requirements
- Explore Security roadmap
- Demonstrate benefits of SOAR and advanced SIEM technologies

Step 2: **Discover**

- Deliver workshop and knowledge transfer
- Analyse and discover gaps
- Consider vendors and offerings

Step 3: **Recommend**

- Align appriopriate technologies to create solutions
- Provide a bespoke solution recommendation report to assist with business cases

What you can expect

- ✓ Interactive 1:1 Session
- ✓ Expert Advice and Guidance
- ✓ Can support multiple stakeholders
- ✓ Sessions run remotely or in person
- ✓ 20+ years experience in Security Optimisation

Explore how Bytes can help you on your journey to more secure and efficient way of managing security operations. If you can only spend 10% of your time optimising – let us help.

Enquire about our free Security Operations Review today by emailing tellmemore@bytes.co.uk

See and understand All Network Threats

One of the key concerns raised by organisations in this report was a lack of perceived confidence in detecting threats in their environments, with organisations on average only being 51% confident that they are able to detect and deal with threats quickly and promptly.

A high proportion of respondents (over x%) had real concerns about detecting Ransomware, data loss and theft, account takeover and even basic malware. How can you be sure your SOC isn't missing key network threats? The good news is Bytes can help.

If you are one of the many people who had real concerns about your SOC's ability to detect and respond to Ransomware, basic malware or other malicious activity – Bytes have a free Assessment which can help you understand if you are missing those threats right now.

Gain peace of mind and see all active threats to your Network – both on premise, endpoints and in the cloud - with a free 'Know your Network' Security Assessment from Bytes.

Simple Setup - No Cost

This free Security Review uses the latest threat prevention technology to provide a free, personalised cyber threat report. Get full visibility of previously unseen threats. Plus expert advice on remediating those threats from our accredited engineers, all for free

This non intrusive detection-only Healthcheck will show you exactly what's really happening on your network right now – so you can gain an accurate picture of if you are missing anything in reality – take action on those and then plan in SOC improvements to ensure better detection in future.

Our accredited security engineers analyse your network, collecting and reporting back to you with comprehensive intelligence on active threats in your complete environment - networks, endpoints and mobile devices - covering:

Application Risks
Which applications are used, high risk application usage and exposure areas

Multiple exposure channels
Loss of sensitive data and threats to endpoints & mobile devices

Real time attack statistics
Exactly how adversaries are attempting to breach your network right now

Your Threat Landscape
The number of malware infections, intrusion attempts and bot attacks

Remediation Recommendations
Key areas to focus on immediately to reduce your risk exposure

Use this free Review to find out what's really happening with your network traffic right now, identify visibility gaps within your SOC and map out steps to make improvements in the places within your SOC which will achieve most tangible, immediate benefit – all with no cost or resource required from your already stretched Operations Team.

About Bytes

Bytes provides leading insights, expertise and practical help to over 3,600 organisations nationwide. We enable effective and cost-efficient technology sourcing, adoption, security and management of software, hardware and cloud services.

Our UK business began in 1982 and has grown profitably each year to reach a turnover in excess of £500m, making us one of the largest software services and solutions businesses in the country.

The most important aspect of our business is our people. We value initiative, teamwork and achievement. Together, we focus on providing the highest levels of service so we can deliver our ultimate goal – customer satisfaction and success.

Our customers include leading brands across retail, media, finance, manufacturing, legal, healthcare and the public sector.

We work closely with the majority of IT vendors and are delighted to regularly receive honours from them in addition to being named a Sunday Times Best Company to Work For 2020.

About Exabeam

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time.

Security organizations no longer have to live with missed distributed attacks, unknown threats, and manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can use behavioral analytics to detect attacks, automate investigation and incident response, and reduce storage costs. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures. For more information, visit www.exabeam.com.

About Palo Alto Networks

Palo Alto Networks, is a global cybersecurity leader that provides technology to help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration.

By delivering an integrated platform and empowering a growing ecosystem of partners, they are at the forefront of protecting tens of thousands of organisations across clouds, networks, and mobile devices.

To understand how Bytes can help you develop and enhance your Security and Security Operations Strategy, get in touch and start a conversation today.

BYTES | Smarter together

UK Head Office

Bytes House
Randalls Way
Leatherhead
Surrey
KT22 7TW

T 01372 418 500
E tellmemore@bytes.co.uk
W www.bytes.co.uk