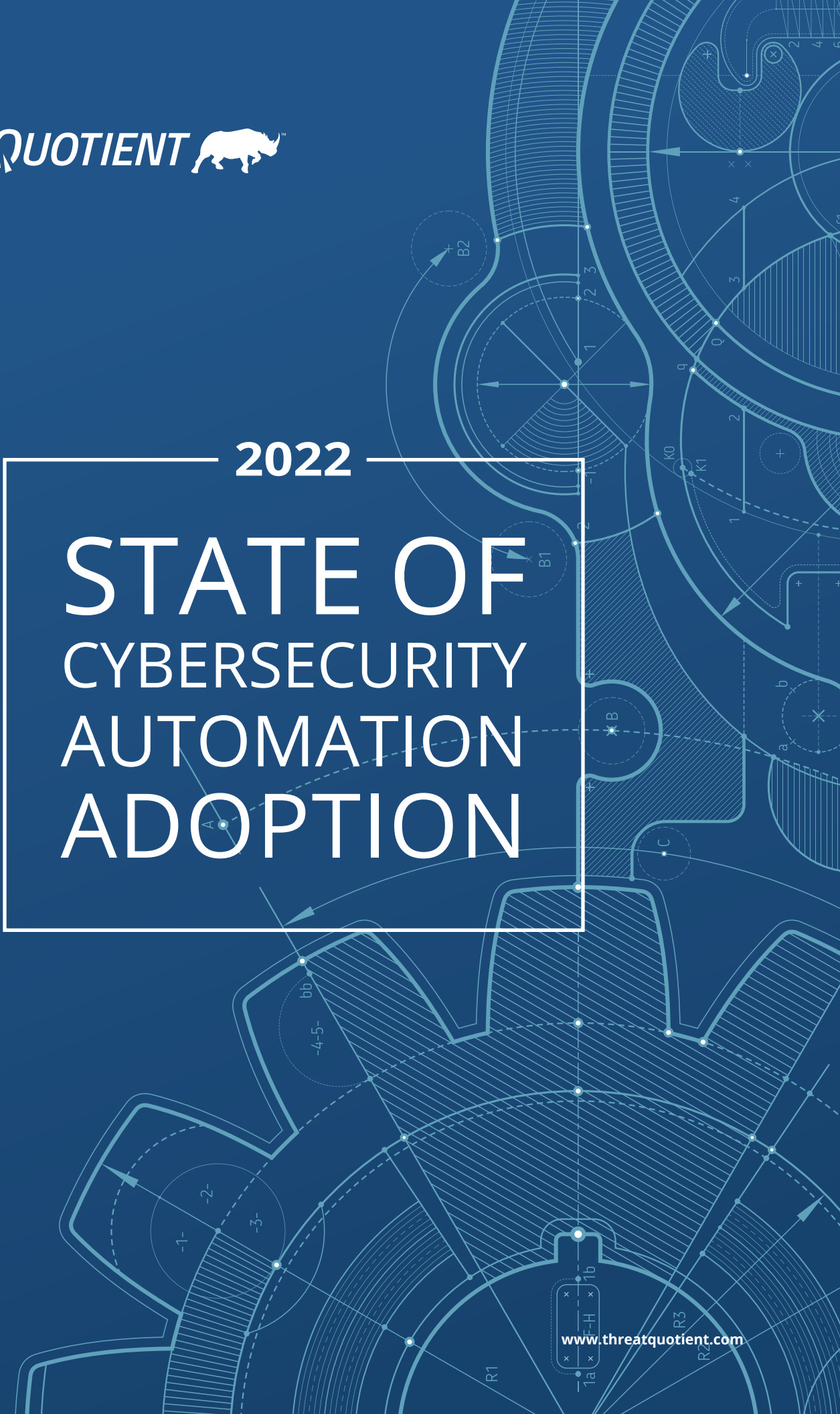
THREATQUOTIENT

2022

STATE OF CYBERSECURITY AUTOMATION ADOPTION



www.threatquotient.com

CONTENTS

2 Introduction
2 Methodology
3 Foreword
5 High Level Findings
8 Vertical Market Snapshot
10 Regional Snapshot
12 Role Based Snapshot
14 Recommendations
15 Questions Responses

INTRODUCTION

This research was conducted to build on the findings of a survey of senior UK cybersecurity professionals carried out in 2021. The research cohort is expanded to 750 senior executives across the UK, US, and Australia, and the study examines the drivers for implementing cybersecurity automation in today's distributed enterprises, exploring the common use cases, the typical challenges faced, and the barriers to automation adoption. The thorny topic of measuring automation ROI is explored and the 2022 report also identifies the level of cybersecurity automation maturity in enterprises. It looks at how the rise of Extended Detection and Response (XDR) is affecting organizations' appetite for automation, and the extent of board-level interest in cybersecurity reporting.

Read this report to understand how CISOs and senior cybersecurity professionals are approaching the challenge of securing the extended enterprise in an intense and complex threat and operational environment. Which automation use cases are working, and which could benefit from more focus?

METHODOLOGY

Leading security operations platform innovator, ThreatQuotient, commissioned a survey, undertaken by independent research organization, Opinion Matters, in July 2022. 750 senior cybersecurity professionals in the UK, US and Australia from companies employing 2,000+ people from five industries took part, including: Central Government, Defense, Critical National Infrastructure - Energy and Utilities, Retail, and the Financial Services Sector.

FOREWORD

The intense and complex cyber threat landscape, coupled with a persistent shortage of skilled security professionals, continues to exert significant pressure on cybersecurity teams. Increasingly, cybersecurity automation offers a solution that enables a more effective security and risk function today, and acts as a foundation to support the protection of the fast-evolving security frontiers of tomorrow.

As businesses and public sector organizations continue to build more agile, distributed working environments alongside highly personalized customer journeys, they must get smarter and more efficient about protecting the data and infrastructure on which they depend. The sheer volume of data generated and the escalation in potential attack vectors mean this cannot be a purely manual undertaking; automation is essential. Our 2022 State of Cybersecurity Automation Adoption research finds that organizations are working to automate various elements of their security strategy and are progressing through different levels of maturity. However, they face challenges along the way. There is evidence that technology complexity, skills shortages, and a lack of senior buy-in are acting as a brake on adoption. Additionally, we identified differences of opinion among the various roles that influence cybersecurity strategy and tactical approach.

Worker well-being and retention forms part of ROI calculations

Alongside the productivity, efficiency, and security benefits sought from cybersecurity, automation is arguably an equally important benefit for employee well-being. By allowing automation to shoulder the burden of time-consuming manual monitoring, identification, triage, and prioritization, analysts can focus on more rewarding higher value activities. This reduces the prospect of burnout or boredom and eliminates the risk of errors resulting from either state. In an employment market where retaining employees is becoming a core challenge and the cost of churn in security teams is significant, using automation to make life more fulfilling is paramount. This is reflected in the way that organizations assess the ROI of their automation programs, with our research finding that qualitative factors around resource management and employee satisfaction are more commonly used than quantitative metrics.

Board focus varies but is generally rising

We also explored the extent of board-level interest in cybersecurity and how this has changed over the past year. Surprisingly, more than one in four respondents say that board level interest in cybersecurity has remained the same or diminished, suggesting that for these organizations the issue is subordinate to other concerns. Certainly, boards have a lot on their agenda with economic challenges, supply chain issues, and regulatory changes all clamoring for attention. Nevertheless, 69% of respondents are facing demands for more frequent and detailed reports, adding to the pressure on senior security executives to demonstrate a robust and coherent cybersecurity strategy.

XDR and automation may be uneasy bedfellows

As the industry matures, we are seeing the shape and scope of cybersecurity automation evolve. At the same time, XDR has become a hot topic in the industry and there has been convergence between the two. However, our research shows that this is not necessarily a match made in heaven. While the majority of respondents have either already deployed XDR, or are planning to do so, one in five respondents say that their willingness to automate cybersecurity has reduced since they deployed XDR. This points to the realization that XDR is not necessarily a silver bullet that can be implemented at the touch of a button, but is more complicated. Applying effective automation to XDR implementations may still be somewhere down the line for organizations that need to walk before they can run.

With organizations largely recognizing the importance of automating cybersecurity processes, our research sheds light on why their efforts may not be succeeding in the way they anticipate, and helps define areas – from siloed departments to technology complexity – to be addressed in order to improve future outcomes.

Here at ThreatQuotient, we know that data-driven automation enables security operations teams to elevate the security posture of their organization confidently and consistently while addressing resource constraints and employee well-being. Our recommendations will assist organizations in avoiding the pitfalls and reaping the rewards of effective cybersecurity automation.

We hope you find this report interesting and valuable.

HIGH LEVEL FINDINGS

68%

say automation is important

98%

have increased their automation budgets

97%

experienced problems

21%

say technology issues are preventing automation

The importance of cybersecurity automation and the desired benefits

Cybersecurity automation is important to senior cybersecurity professionals, with more than two-thirds saying it is very or somewhat important. The key drivers for adopting automation are a desire to improve both the efficiency and standard of cybersecurity within the business. In the UK, respondents are also seeking to address the skills shortage, while in the US regulatory compliance demands are also a driving factor.

Threat Intelligence Management and Incident Response are the most popular automation use cases, but alert triage is being overlooked

Organizations are most likely to already be automating threat intelligence management and incident response (IR), with phishing analysis and vulnerability management not far

behind. Nevertheless, in absolute terms only around one-quarter of respondents are automating these processes in each case, so there is definitely room for improvement. Surprisingly, only 18% of respondents are automating alert triage, despite this being a potential route to reducing the burden of manual review and prioritization. Of course, not all alerts are routine issues suitable for automated responses, and this variation in the severity of alerts may be behind a level of reticence to deploy automation in this case.

Cybersecurity automation still faces barriers to adoption

Implementing automation is not plain sailing, with 97% reporting difficulties in rolling out automation initiatives. The most commonly cited challenge is technology issues, which often arise when automation is overlaid on a heterogeneous environment comprising multiple legacy toolsets. Skill shortages and lack of management buy-in are also preventing automation adoption, while further down the list siloed departments and a lack of trust in outcomes are also problems preventing the effective rollout of initiatives.

The most commonly cited challenge is technology issues, which often arise when automation is overlaid on a heterogeneous environment comprising multiple legacy toolsets.

Over time, however, the barriers to implementation do seem to have dropped. When comparing these survey results to last year's UK findings, the proportion of respondents reporting problems in each area has significantly reduced.

Most organizations are less than mid-way to maturity

Asked to identify their automation maturity on a scale of five different levels, the majority of organizations (62%) rate themselves at level two or three.

Those at level two are using some intelligence feeds, but do not have a SOC or SIEM in place and cannot link threats to their strategic position. They have limited resources to support their security practice. At level three, organizations have an established cybersecurity operations practice with dedicated personnel, can curate intelligence feeds and relate threats to organizational environment or events, but are mostly reactive and time to detection is longer than ideal.

Coupled with the challenges organizations are facing in terms of adopting automation, it seems that moving up through maturity levels is a challenge. It is likely to be a slow process requiring everything from financial investment to structural and culture change to reduce silos and promote an approach that cuts across the whole business.

Budgets are rising

There is good news on the subject of investment, however, with 98% indicating that the automation budget is increasing, although many are eating into other departmental or technology budgets to achieve this. A notable proportion (30%) are allocating unused headcount budget, which is an intelligent initiative if it boosts productivity and efficiency when skills are in short supply.

Board interest is rising too – for the most part

69% of those surveyed are experiencing greater interest from the board; 38% are being asked to deliver more frequent and more detailed reports. A further 21% are being asked to report more regularly, although detail has not increased, while another 10% are being asked for more detail in each report they deliver. Nevertheless, there is a notable proportion – 22% – who have not seen any change in board interest; 7% say interest has actually decreased. While boards have a lot on their radar at present with supply chain issues, political instability, and economic turmoil demanding their fair share of focus, prioritizing these at the expense of cybersecurity awareness is high risk. All those preceding factors are also having an escalatory impact on cybersecurity – in fact they are frequently symbiotic.

Qualitative measures are marginally ahead of quantitative metrics when it comes to assessing ROI

Determining the ROI of cybersecurity automation projects has been highlighted as one of its more challenging aspects. A recent SANS cyber threat intelligence (CTI) survey found that a high percentage of organizations are struggling to measure CTI program effectiveness, making it difficult to bid for more resources to move to a higher maturity level. Asked how they are assessing ROI, the most popular method was how well the organization is managing its resources, including staff and budget (chosen by 42%). This is followed by how well the business is doing on team management such as employee satisfaction and retention (39%). Quantitative metrics on how well the job is being done came third, with 36.5% saying they use these to evaluate ROI.

While the use of qualitative aspects underscores the impact automation has on improving employees' experience, quantitative metrics are more objective and can be useful in reporting to the board when making the case for further investment.

XDR

The relative novelty of XDR and the likelihood that most respondents remain in the early stages of implementation was evident in the responses to questions about its impact on willingness to automate cybersecurity. The picture is mixed, with some indication that organizations that have already deployed XDR are now less willing to automate. Now that XDR is rolling out in earnest, this could indicate that the complexities involved are surfacing. It will be interesting to see how these sentiments change in the years ahead.

VERTICAL MARKET SNAPSHOT

Financial Services companies are most likely to consider cybersecurity automation important (75%), reflecting the fact that this industry typically faces the most threats. Respondents in Retail were most likely to say cybersecurity automation is not important (20%), with only 55% saying it is important. Interestingly, when we compare Retail responses in the UK with last year's survey, we find perceived importance has dropped significantly, from 82% in 2021 to only 50% this year.

ThreatQuotient Take:

The Retail sector was turbulent during the COVID-19 pandemic, with a rapid pivot to online sales leading to record revenues for many. This put the spotlight on cybersecurity and the impact attacks would have on resilience and revenues, accelerating the need for automation, especially in a market short on cybersecurity skills. Now, the environment has changed; retailers are facing the prospect of recession and belt-tightening, so there's less room for new automation investment. Bearing this out is the fact that Retail respondents are the least likely to be getting net-new budget, and most likely to say budgets have remained static.

Increasing efficiency is a key driver for automation in the Financial Services industry (37%), while 30% of Retail respondents see automation as a solution to the skills shortage. Critical National Infrastructure respondents see improving/maintaining cybersecurity standards as a key driver (39%). Central Government respondents are most commonly driven by regulation and compliance (29%).

In terms of cybersecurity automation adoption, Critical National Infrastructure and Financial Services organizations are ahead of their peers and more likely to be automating processes overall. Notably, respondents from the Defense sector were far less likely than other sectors to automate vulnerability management (16% doing so versus 27% on average among other sectors). However, they were more likely to be automating threat hunting (30% versus an average of 24% in other sectors).

When it comes to barriers to adopting cybersecurity automation, Central Government (19%) and Defense organizations (21%) find the issue of siloed departments to be their biggest problem, while budget (21%) and skills (23%) are preventing automation in Financial Services. Technology is the biggest blocker for Critical National Infrastructure respondents, with 27% citing this as an issue, and trust in outcomes also causing problems, with 21% of respondents in this sector raising it as a barrier. For Retail respondents, a lack of skills is holding them back (19%).

There is some consensus around the problems being faced during automation implementation, with "technology" a common problem. For Central Government the top issue is "breaking systems", perhaps indicating the level of legacy technology in the sector. Similarly, technology issues are the top challenge for Defense organizations, while in Critical National Infrastructure the skills shortage is by far the biggest issue, affecting 23%. In Retail and Financial Services, management buy-in is the main issue affecting implementation.

Financial Services is an outlier, with 8% reporting no issues in implementing cybersecurity automation.

Average level of cybersecurity operations maturity	
Central Government	2.63
Defense	2.84
Critical National Infrastructure	2.79
Retail	2.69
Financial Services	2.66

Cybersecurity operations maturity scale:

In terms of overall cybersecurity operations maturity, when asked to rate their maturity from 1 – 5, the Defense sector has the highest percentage at level 5 (9%), while Central Government has only 3% claiming this level of maturity. That said, the average maturity level across sectors is fairly comparable, between 2.63 and 2.84.

Interestingly, boards at Retail companies are showing notably lower demand for data on cybersecurity performance. One-quarter (25%) say interest has not increased and 12% say it has decreased. Again, this may be down to the turbulence affecting the sector diverting board attention away from security.

The split of budget sources is broadly similar across all vertical sectors. Financial Services companies are more likely than average to be allocating unused headcount budget to cybersecurity (34%). Retail companies are less likely than others to be getting net-new budget (29%), again reflecting the drop in focus on cybersecurity in this sector.

The Critical National Infrastructure sector is more likely than average to be increasing its cybersecurity automation budget due to diverting budget from other tools (37%). As closer integration of IT and OT continues, it is likely that organizations are understanding the value of automation to manage and triage security issues.

Where ROI metrics are concerned, the Defense sector leads the others in choosing employee satisfaction/retention as the most important metric, selected by 43%. This sector faces far higher employee screening requirements and a longer recruitment cycle, making it important to keep employees once they have them onboard. Retail respondents also chose employee satisfaction/retention as its most important metric (39%).

In the Critical National Infrastructure sector, however, resource management was the main success metric, chosen by 53% of respondents and reflecting the sector's culture of efficiency. This was echoed in Financial Services and Central Government.

REGIONAL SNAPSHOT

We surveyed cybersecurity professionals in the UK, US, and Australia to explore their different views on automation.

70% of UK organizations say cybersecurity automation is important to their organization. This is a drop from last year when 77% rated it as important. 65% of US respondents and 68% of Australian respondents agree that automation is important to their business.

In the UK, increasing productivity is the main driver (29%) for automation, the same as in last year's survey. The second most important driver for the UK is addressing the skills shortage through automation (25%), followed by increasing efficiency (24%). In the US, the main driver is meeting regulatory compliance demands (27%), which is almost equally important as increasing efficiency and improving/maintaining cybersecurity standards. In Australia, the need to improve/maintain standards is the most important driver (37%), followed by increasing efficiency and regulatory compliance (both 36%).

Respondents from Australia are automating more cybersecurity use cases than counterparts in the UK and US. The most popular application in Australia is phishing

analysis, which is automated by 36% compared to only 19% of US and 22% of UK respondents. In the UK the most popular use cases for automation are threat hunting and threat intelligence management (both 24%) while in the US vulnerability management and incident response tie at 24%.

Barriers to cybersecurity automation differ. For US and UK respondents, "technology" is the dominant challenge, affecting 18% and 21% respectively, while in Australia, management understanding and buy-in alongside trust in outcomes are the main barriers (affecting 23%). Overall, however, barriers seem to have lowered: last year, 40% of UK respondents said budget was an issue, compared to only 16% this year. 25% said time was a problem, compared to 14% this year. 32% said resources were a problem, compared to 15% this year, and 31% said management buy-in was an issue, compared to 17% this year.

Compared to last year, the issue of lack of trust in outcomes has reduced among UK respondents. 41% said they had encountered this as a problem in 2021, compared to 12% in 2022. In fact, while overall more UK respondents said they had experienced problems, the frequency reported for each issue was lower – the only problem that rose in frequency was siloed departments, which rose from 12% in 2021 to 15% in 2022.

Most common use cases:

Phishing Analysis (Australia)

Threat Hunting & Threat Intelligence Management (UK)

Vulnerability Management & Incident Response (US)

In Australia, however, lack of trust in outcomes is significantly more of a problem during implementation than in the US and UK. Almost one-quarter (23%) say it is a problem, around twice the level in the other regions. Australian organizations are experiencing more problems across the board, with 24% suffering breaking systems, 23% lacking management buy-in, and 21% having technology issues. In contrast, only between 14% and 17% of US and UK respondents are having these problems.

Despite these issues, Australian respondents rate their organizations as more mature in cybersecurity operations, with an average region maturity of 2.85. In the UK, 43% of respondents rate maturity at level 2 or lower, a figure that rises to 51% of US organizations. However, the US has the highest number of organizations at level 5, with 9% saying they have reached full cybersecurity operations maturity.

Increases in board interest in cybersecurity are highest in the US, where 71% are being asked for either more frequent and/or detailed reports. Australia is slightly behind at 70% and the UK at 68%. However, 30% of respondents in both the UK and Australia, and 27% in the US say board interest has not increased.

98% of UK organizations are getting increased budget, compared to 95% of both US and Australian organizations. Australian companies are most likely to be getting net-new budget (46%), while the biggest source of budget for US organizations is through reallocation of unused headcount (29%). In the UK, the most common source of budget is through reallocation from other tools (29%).

On the subject of ROI, the US and Australia are more focused on how well they are managing their teams, with 40% and 43% respectively choosing this metric, compared to the UK where only 35% selected it. The UK is more focused on how well resources are managed (40%).

The US is ahead on XDR implementation, with 55% saying they have already adopted it. 48% of Australian and 44% of UK organizations have rolled out XDR.

ROLE BASED SNAPSHOT

Across the research cohort there was significant variation in how the different roles viewed the issue and challenges of automation. This underlines the fact that often internal politics and differing motivations can act as a brake on investment and the implementation of new technologies.

Over three quarters (76%) of Heads of SOCs and Heads of IT Security Solutions/ Architecture say cybersecurity automation is important, while only 60% of Heads of CTI, 62% of CISOs, and 64% of Heads of IR say it is important. Incident responders are also most likely to say automation is not important (16%), which perhaps reflects a perception that IR must be human-centered and tailored to the situation.

Improving/maintaining cybersecurity standards is a clear driver for Heads of IT Security Solutions/Architecture (46%) and for Heads of IR (43%). Heads of CTI are more focused than other roles on solving the skills shortage through automation (37% compared with an average among other roles of 22%). For MSSPs increasing efficiency is the key driver (53%).

Heads of SOCs are less likely than those in other roles to automate cybersecurity processes, perhaps favoring hands-on approaches. However, it is notable that CISOs are also far less likely than other roles to say their organization automates key cybersecurity processes. As an example, only 19% of CISOs say they automate threat intelligence, whereas 46% of Heads of IT Security Solutions/Architecture do.

There are variations between different roles in their perception of barriers. CISOs are less likely than other roles to say management buy-in is an issue; instead, they say the biggest issue is siloed departments. They may not appreciate how intelligent automation can break down siloes by automating actions and ticket-raising in multiple teams to create a coordinated response. There is an opportunity for stakeholders in other roles, who are struggling to get management buy-in, to speak to overcoming this pain point when building their business case to the C-Suite.

ThreatQuotient Take:

Heads of IT Security Solutions/Architecture are having the most issues with management buy-in (37%) compared with the other job roles (18%). This may be due to the different nature of the roles. Heads of SOCs, IR and CTI are very hands-on in the implementation of automation and solving issues daily, gaining buy-in as they report on progress. In contrast, solutions architects tend to be more theoretical and future-focused; they're seeking to design an ideal future state. It is possible that they feel cybersecurity automation is not being adopted in the strategic way they want it to be. IT solutions architects are also more likely than other roles to say that budget is an issue, possibly indicating that they have concerns about the longer-term funding of automation projects. Certainly, there is a disconnect across different role types on the challenges and barriers to automation.

Heads of SOCs are least likely to say that a shortage of skills is a barrier, with only 10% reporting this as a problem, compared to an average of 21% across other roles.

In terms of role, Heads of SOCs and Heads of IT Security Solutions/Architecture are more likely to be experiencing increased demand for reports, with 46% saying they need to deliver more frequent and more detailed reports.

Heads of IR are the most likely to report getting net-new budget, with 51% stating this compared to an average of 36% across the other roles. This may reflect awareness of how high-profile attacks can impact the organization and the need to dedicate resources to rapid and effective response. Heads of IR are also more likely than others to get budget from unused headcount (40% compared with 31% among other roles).

The roles are broadly in agreement that how well they are managing resources such as staffing, efficiency and budget is the best metric for determining ROI. The only outliers are Heads of IT Security Solutions/Architecture, who say that how well the team is doing the job in terms of mean time to detection and resolution is the main metric they use. Again, this aligns with the more strategic viewpoint of this audience.

Heads of IT Security Solutions/Architecture, say that how well the team is doing the job in terms of mean time to detection and resolution is the main metric they use. Again, this aligns with the more strategic viewpoint of this audience.

RECOMMENDATIONS

While the research shows that organizations have certainly made progress over the last year when using automation to manage routine work and improve overall cybersecurity maturity, many teams still report challenges with automation including technological complexity, skills shortages, and a lack of buy-in from management. Based on the research findings, here are six recommendations for security professionals responsible for automation. Consider these recommendations when working on initiatives to improve the effectiveness and efficiency of cybersecurity automation:

1. **When deploying or maturing cybersecurity** automation, choose use cases that are proven to show value by saving time and/or improving the effectiveness of security procedures; popular choices include threat intelligence management, incident response, phishing analysis, and vulnerability management.

2. **Context is king.** What is true for cybersecurity in general, is equally important for automation. A data-driven approach ensures that automation is focused on relevant and high priority events while data is captured to provide context for further analysis and continuous improvement.

3. **Simplify complexity** and address skill shortages by adopting cybersecurity automation platforms with low- or no-code interfaces. When skills are not available or cannot be developed in-house, look to MSSPs who place importance on cybersecurity automation – 85% say it is important – reflecting their need to manage high volumes of data and alerts on behalf of customers and to leverage insights rapidly and effectively.

4. **Remember that automation is a spectrum** ranging from simple, atomic-level tasks to complex, multistep playbooks with built-in decision logic. It's important to choose a cybersecurity automation platform that accounts for the full spectrum of use cases.

5. **Gain management support** for automation by defining clear metrics for success and measuring progress along the way. Balance the quantitative impact with qualitative factors including employee satisfaction and retention.

6. **Standardize on cybersecurity** automation platforms with open versus closed architectures to ensure interoperability across the widest range of security tools and extensibility when working with emerging technologies such as XDR.

QUESTIONS ANS RESPONSES:

Q1. How important is cybersecurity automation to your organization?

The majority of survey respondents have cyber security automation firmly on the agenda. More than two thirds of respondents (68%) say cybersecurity automation is very (25%) or somewhat (43%) important to their organization. Respondents from the UK are most likely to say it is important (70%) although this is a drop on the 77% who said it was important in the previous survey.

Just over one-quarter (26%) are ambivalent about cybersecurity automation, while for 9% it is not important.

Overall, the perceived importance of cybersecurity automation tends to increase the larger the organization, which is logical. The exception is organizations with 4,000-6,000 employees in the UK, where there is a notable dip with just 49% rating it important and 15.5% rating it not important. This may align with the fact that organizations of this size are likely to be using MSSPs to handle security requirements and therefore have less exposure to the need for automation.

Q2. What, if any, are the main drivers behind your organization's need to adopt more cybersecurity automation? (Select up to 3 top drivers)

Every respondent, whatever their role, region or market sector, was able to identify at least one primary driver for adopting more cybersecurity automation. Organizations are almost equally driven by the desire to improve efficiency (29.1%), improve and/or maintain cybersecurity standards (28.9%), and comply with regulations (28.8%).

Increasing productivity is also an important focus, selected by 28%, while one-quarter see automation as a key route to addressing the skills shortage.

The larger the organization, the more importance it places on regulation and compliance as a driver for automation. 35% of respondents from companies with more than 10,000 employees cited it compared to only 28% of those with 2,000-3,999 employees.

Q3. What, if any, cybersecurity processes/use cases do you automate today in your organization? (Tick all that apply)

The top cybersecurity processes/use cases automated by organizations overall are threat intelligence and IR (26.5% each). This is followed by phishing analysis, vulnerability management and threat hunting.

Interestingly, relatively few are automating alert triage – 18% (this is heavily weighted by Australia, where 27% are using it. In the UK and US only 13% and 14% respectively automate alert triage.)

ThreatQuotient Take:

Automation can be applied to alert triage, but the extent to which it is used depends on the organization's attitude to alerts and their typical severity score. If an alert is high scoring, the majority of security teams will want to manage it in person; automation may be used for some initial enrichment and context, but for the most part teams will want to be hands-on. If this is a common scenario it is worth exploring the potential of atomic automation, where individual actions in the alert triage process are automated but not an entire playbook. This allows analysts to hand off some of the heavy lifting but still take the lead on evaluation.

Once again, larger organizations are generally making greater use of automation across the board. 41% of those with 10,000 or more employees are automating threat intelligence, for example, compared with 24% of companies with 6,000-9,999 employees.

Q4. What, if anything, is preventing your organization from applying cybersecurity automation?

"Technology" is the top factor preventing organizations from applying cybersecurity automation (21%), followed by skills (17%) and management understanding/buy-in (17%). However, lack of trust in outcomes, budget, siloed departments, breaking systems, bad decisions, and resources all featured in responses, showing that the reasons are complex and disparate, probably depending on the cybersecurity maturity of the organization.

Interestingly, lack of trust in outcomes has dropped as a barrier. In last year's UK survey this was cited as a problem for 41% of respondents; now it is at 12% in the UK and 14% across all territories.

ThreatQuotient Take:

Last year, 37% on average had already automated key processes, and 45% were planning to do so in the coming year. Now that the additional 45% are getting hands-on with automation and rollout is maturing, more practical challenges such as technology integration and skills shortages are being felt. Pre-deployment concerns were more conceptual around issues like trust in outcomes. Now teams are more focused on how best to apply automation to heterogeneous environments and legacy tools. It is here where solutions that simplify set-up of key use cases and use no-code to make automation accessible to a wider group of personnel can help overcome barriers and accelerate effective automation.

Q5. Has your organization encountered problems/issues when implementing cybersecurity automation, and if so, what problems/issues have arisen? (Tick all that apply)

An incredible 97% of respondents have encountered problems implementing cybersecurity automation overall and the figures are broadly similar across all three countries. In the UK, 98% said they had experienced problems, up from 92% who said the same one year ago.

It is clear that the road to automation does not run smoothly. Again, this may be a sign of the maturing market; as more adopt automation, more experience challenges.

The most common problem is management understanding/buy-in (19%), followed by technology issues (18%) and lack of skill (16.5%). There is a broad spread of issues, however, including lack of trust in outcomes, which was a problem for 16% overall, though this represents a fall from the 41% in the UK who expressed concerns about this issue in 2021.

Q6. Reading the following five descriptions of cybersecurity operations maturity below, what stage would you say reflects / is closest to reflecting what your organization has achieved? (Select best match)

The overall level of cybersecurity operation maturity among respondents, on the scale of 1-5, is 2.72. The majority (63%) rate themselves at level two (31%) or level three (31.5%). 19% are at level four and just 5% are at level five. 13% are immature, recognizing the need to establish a cybersecurity operations capability but not having the resources to do so.

Average maturity by region	
UK	2.71
US	2.61
Australia	2.85

These are subjective ratings, and it is interesting that Australian respondents rate themselves as more mature than their US or UK counterparts.

CISOs, who might be expected to have the best overview of overall maturity, rate their organizations least mature, at 2.5 on average. Heads of SOCs, Heads of CTI and Heads of IR are more bullish about their position, rating it at 2.74, 2.98 and 2.84 respectively. Heads of IT Security Solutions/Architecture are more positive, giving an average rating of 3.

Average maturity by sector	
Central Government	2.71
Defense	2.61
Critical National Infrastructure	2.85
Retail	2.69
Financial services	2.66

As discussed previously, 9% within the Defense sector perceive they have the highest level of maturity, while only 3% in Central Government report to be at level 5 maturity. That said, the average maturity level across sectors is fairly comparable, between 2.61 and 2.85.

Q7. If it is required at all, has the detail/frequency of cybersecurity reporting (e.g., threats and risks, investigations, budget, etc.) required by your company's board of directors changed in the past 12 months?

Overall, cybersecurity professionals are facing demands to produce more frequent AND more detailed board reports; 38% confirm this. A further 10% say only detail has increased and another 21% say only frequency has increased. Therefore, in total 69% of respondents are being asked for a higher level of reporting compared to a year ago. The US is feeling it most, with 40% reporting a need for more detailed and frequent reports and 71% overall being asked for enhanced reports.

Concerningly, however, a notable proportion (22%) say that there **hasn't** been an increase in board interest in cybersecurity, and 7% say board interest in cybersecurity reporting has **decreased**.

Ultimately the general level of threat and the potential impact of cyberattacks means boards should be demanding more frequent and detailed data on the business's cybersecurity posture. It should be a pillar of risk management and oversight, so although it is positive that we are seeing demands for more information from the board, we ought to see this increase still further. Cybersecurity teams need to be prepared for more requests and demands for greater detail and boards should aim to move from a reactive stance to a more proactive position, working with cybersecurity teams to understand emerging threats.

Q8. To what extent, if at all & how, has your budget for cybersecurity automation changed in the past year?

The good news is that for most organizations (97.5%) cybersecurity automation budgets have increased – very few report decreases – and funds are coming from a range of directions. 34% said they are getting net-new budget. Companies are also diverting resources from tools such as SIEM (29%) and security teams are gaining budget diverted from outside their department, e.g. IT Ops (32%). 30% have allocated unused headcount budget to automation – perhaps due to the skills shortage and difficulties in recruiting personnel in the current environment. Automation is the pragmatic solution to recruitment challenges by reducing the headcount needed to achieve the same result and handing over repetitive, low-level tasks to robotic process automation.

The biggest organizations (with 10,000+ employees) are likely to be getting more net-new budget, with 43% reporting this compared to only 27.5% of organizations with 2,000-3,999 employees. Smaller organizations are also more likely to be getting budget from other teams, highlighting the balancing act that smaller businesses have to undertake to allocate scarce resources where they are best needed.

Q9. What, if any, are the metrics you use to measure cybersecurity automation ROI/KPIs? (Tick all that apply)

The most popular way of measuring cybersecurity automation ROI is by analyzing "How well we are managing our resources (e.g., staffing/efficiency effectiveness, budget)" (42%). 39% say they measure how well they are managing the team, looking at issues such as employee satisfaction and retention. When automation is effectively deployed these should increase, as individuals spend less time on repetitive, low-value activities and more on work that has a clear benefit to the business. This is evident among ThreatQuotient customers, who want to get analysts focused on what's important.

37% overall look at how well they are managing to do the job in terms of mean time to detection and response. This may be tougher to measure than the other metrics, involving a lot more complexity than the others.

The larger the company, the more metrics are being used overall to measure the success of automation, which reflects the fact that they are typically subject to higher reporting requirements in general. For the very largest companies with 10,000+ employees, the issue of employee satisfaction is the top metric, selected by 56% of respondents. Interestingly, employee satisfaction is also the most important metric in the smallest companies (40%). This is telling, as recruitment can be most challenging at both ends of the scale and therefore companies are making more efforts to retain employees.

Q10. Recently we have seen some convergence between XDR and cybersecurity automation. Are you considering or have you implemented XDR in the last 12 months and how, if at all, has this impacted on your willingness to automate incident response this year compared to last year? (Select best match)

Overall, 49% of respondents have implemented XDR and a further 44% are considering doing so.

Among those who have implemented XDR, 19% say there is less willingness to automate incident response than previously, 18% say willingness to automate is the same, and 12% say willingness has increased. Ultimately, there is not a clear tie between XDR implementation and willingness to automate.

ThreatQuotient Take:

Automation is one of the key capabilities that you get from XDR. The bigger benefit is integration across all tools, but automation is close behind. This slight drop in willingness to automate once XDR has been implemented is curious – perhaps teams are finding that it is not quite as simple as they first thought so are focusing on getting the integration right first, before moving to automation as the next stage in the XDR maturity curve. Certainly, solutions that make automation easier to apply in parallel with XDR can help to solve some of these concerns.

However, this is all very new and there are many different viewpoints on XDR implementation and how automation fits into that. It will be interesting to track this over the coming year and see how attitudes change as implementation matures.

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage, vulnerability prioritization and threat intelligence management. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit **www.threatquotient.com**.