THREATQUOTIENT

2023

STATE OF CYBERSECURITY AUTOMATION ADOPTION

www.threatquotient.com

CONTENTS

2 Introduction
2 Methodology
3 Foreword
5 High Level Findings
8 Regional Variations
10 Vertical Snapshot
13 Role Based Comparisons
15 Recommendations
17 Question Responses

INTRODUCTION

This is the third edition of ThreatQuotient's annual survey of senior cybersecurity professionals, exploring the topic of cybersecurity automation adoption. Seven hundred and fifty senior executives in the UK, US, and Australia shared their views on the progress they are making toward adopting cybersecurity automation, its key use cases, and the challenges they face. In addition to identifying trends over time, this year's study explores wider issues such as the critical features cybersecurity professionals want to see in automation solutions, the topic of wellbeing among cybersecurity teams, and how it can be improved.

Read this report to understand how CISOs and senior cybersecurity professionals are handling the incorporation of cybersecurity automation into their strategies to protect the complex, extended enterprise – and their analyst teams – from the pressures of escalating cyber threats.

METHODOLOGY

Leading security operations platform innovator, ThreatQuotient, commissioned a survey, undertaken by independent research organization, Opinion Matters, in June 2023. Seven hundred and fifty senior cybersecurity professionals in the UK, USA 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 pressure on cybersecurity teams shows no signs of abating. While the global health crisis is behind us, the past 18 months have brought a worldwide economic uncertainty and geopolitical tension at a level not seen for decades. The resulting energy crisis, supply chain impacts, and effects on employment are sending shockwaves throughout the physical and digital world, and – wherever there is disruption – cybercriminals and nation-state actors are always on hand to capitalize on the situation. Right now, they are leveraging new tools, such as automation and generative artificial intelligence (AI), to make attacks more sophisticated and deceptive. As the volume and variety of cyber threats increase exponentially, and skilled cybersecurity workers remain in short supply, senior cybersecurity leaders face a relentless resource challenge: how to protect the organization in an environment where budgets and personnel are under pressure.

Over the three years that we have undertaken this survey, we have tracked the adoption of cybersecurity automation as a solution to this problem. Our 2023 State of Cybersecurity Automation Adoption research finds that organizations are leaning on automation to handle a growing percentage of cybersecurity use cases with the goal of increasing efficiency, responding to regulation and compliance requirements, and increasing productivity. Overall, they consider automation to be important in their organization, and they are continuing to commit budget to automation programs – even though they are having to cut back in other areas to do so. However, our study also shows that the problems highlighted in previous years remain – in fact, they have grown. Every respondent said they had experienced difficulties of some kind when implementing cybersecurity automation. These range from a lack of trust in the outcomes of automated processes, slow adoption by users, bad decisions resulting from automation, and a lack of skill among users.

There is undoubtedly a degree of disenchantment around automation evident in this year's study, with a sense that it hasn't yet delivered on its promise. This mirrors the findings of other industry watchers and reflects the fact that the market is still relatively immature. Users are still working to find their feet and implement the solutions that will solve their challenges and deliver the right kind of ROI. At the same time, vendors are continuing to innovate and advance their solutions from both a technical and usability perspective, so they can achieve their potential.

ROI is firmly centered on employee wellbeing

Last year, respondents were divided on the best way to determine cybersecurity automation ROI, but this year strong consensus has emerged. 61.5% say that ROI is measured by how well they are managing the team in terms of employee satisfaction and retention. Less than half that figure (29%) say ROI is determined by how well the solution is performing in security terms.

This points to a signal shift in what organizations view as the "point" of investing in cybersecurity automation – the prime motivation is to improve the experience of employees. By allowing automation to shoulder the burden of lower value, repetitive activities, and release analysts for more interesting and fulfilling work, companies can improve employee satisfaction and reduce churn. The study found that high team member churn rates were among the top three challenges facing respondents in central government and critical national infrastructure organizations. It was also the biggest issue facing Australian respondents and those in a CISO role.

61.5% say that ROI is measured by how well they are managing the team in terms of employee satisfaction and retention.

This finding on ROI has important implications for automation solution vendors, too. Typically, vendors design solutions on the assumption that buyers are looking for conventional ROI based on security, accuracy, efficiency, and productivity gains. However, this finding shows that non-traditional, human-focused measures are equally, and sometimes more, important. With ROI measured on the basis of team satisfaction and retention, vendors need to incorporate the human benefits of their solution into product design and messaging. There are several developments on the horizon that should respond to this need, including the advancements of AI and greater rollout of low and no-code solutions. By improving usability and making automation more accessible for a wider cohort of workers, it should deliver more user satisfaction while simultaneously achieving the accuracy and efficiency it was originally designed for.

Here at ThreatQuotient, we know that data-driven automation can play a key role in helping organizations deal with the technical and human challenges of cybersecurity. Our recommendations will assist organizations in avoiding the pitfalls and reaping the rewards of effective cybersecurity automation.

We hope that you find this report interesting and valuable.

HIGH LEVEL FINDINGS

100%

Have experienced problems when trying to automate cybersecurity

99.9%

Have increased budgets for cybersecurity automation

75%

Say IT cybersecurity automation is important to their organization

61.5%

Measure ROI on the basis of how well they are managing the team and employee satisfaction/ retention

The importance of cybersecurity automation rises overall – but there are signs of disenchantment in some regions

Three-quarters of the cybersecurity professionals surveyed said that cybersecurity automation is important to their organization, with almost one-third (32%) saying it is very important. Respondents from the US and Australia showed a 17.5% and 14% increase respectively in the percentage of respondents rating cybersecurity automation important, up at 82.5% and 82%, compared to last year.

In the UK, however, there has been a decrease of 9%, with 61% saying it is important to their business this year. This drop has been led by financial services, defense, and central government respondents. UK respondents were more likely than those in the US and Australia to say that they had experienced bad decisions and slow user adoption resulting

from their attempts to implement cybersecurity automation and that it "causes more problems than it solves". This has generated a level of dissatisfaction that reflects the maturity of the UK market – earlier automation solutions have proved to be complex and hard to use, which would certainly translate into slow adoption.

Automation is being more widely used across all use cases

Compared to last year, a higher percentage of respondents are automating key areas of their cybersecurity program. The most notable increase is in alert triage – an area where ThreatQuotient research identified an opportunity last year – where 30% are now using automation compared to only 18% in 2022. Overall, respondents are around 5% more likely to be automating processes across the range of cybersecurity activities than they were last year.

Interestingly, vulnerability management and prioritization are now a key use case among 37% of US organizations, and it is also more prevalent among companies larger than 10,000 employees (42.5%) and those in the critical national infrastructure sector (37%). In our experience, these are typically more mature organizations when it comes to automation, indicating that we may see vulnerability management rise up the agenda in other, less mature, organizations in future.

Greater adoption is surfacing greater challenges and a lack of trust is key among them

The result is unanimous: implementing cybersecurity automation is never problem-free. The more organizations use automation, the more challenges they are uncovering. Everyone taking part in the research said they had encountered problems, with the most common troubling area being a lack of trust in the outcomes delivered by automated processes – an issue for 31%. Close behind is "slow user adoption" – which is not surprising if users don't trust what they are seeing. "Bad decisions", such as incorrectly blocking suspicious-looking domain names that are actually benign, or blocking an email to the CEO that turns out to be genuine, and lack of skills make up the top four issues.

In combination, these issues point to an environment where the reality of deploying automation solutions isn't matching expectations. As vendors build new features and functionality into tools, there is a distinct need to focus on usability and transparency, so teams can build confidence and reap the benefits of automation.

Finance, regulatory concerns, and team churn are the top three cybersecurity team challenges

We wanted to get a broader perspective on the issues cybersecurity leaders are facing among their teams and here we found evidence that the macroeconomic picture is having an impact. Almost a quarter of respondents (24%) said "insufficient budget" was in their top three biggest challenges, reflecting the economic pressures facing businesses. The same percentage (24%) pointed to "growing compliance requirements" as regulators increasingly introduce mandatory cybersecurity resilience and recovery requirements into draft legislation and regulations.

High team member churn rate was tied at third among the respondents' concerns, indicating that the general disruption in the employment market that followed the pandemic is affecting cybersecurity teams just as much as other job roles. Employee churn causes problems as departing team members take valuable skills and company-specific expertise away with them, which are hard to replace in the current employment environment. Notably, CISOs rate high team member churn as their most pressing issue – and they are also most likely to say that increasing headcount would have the biggest effect on cybersecurity analyst wellbeing.

Budgets continue to rise, but economic pressures are being felt

All but one respondent reported that their budget for cybersecurity automation has increased, a rise to 99.9% from 98.5% last year. However, compared to last year, budget is far less likely to be net new allocations – only 18.5% had a net new budget this year compared to 34% that had it last year. Instead, budget is being allocated from outside the security team or from other tools. There's a slight drop in budget being reallocated from headcount compared to last year, which may show that businesses are still trying to bolster their security team numbers.

The level of consensus across countries and industries on the budget topic was incredibly strong. Economic headwinds are being felt everywhere, forcing businesses to be creative about how and what they fund. The good news is that cybersecurity automation clearly holds a critical position within the strategies of these businesses, to the extent that they are prepared to cut other budgets to ensure continued investment.

Multiple data source integration, training, and automated reporting tools top the wish list

When selecting cybersecurity automation solutions, organizations primarily want the facility to integrate with multiple data sources – and as the number and format of sources grows, this will surely become more important as teams seek to make sense of increasing volumes of data. Next on the list is training – essential as teams seek to grow their skills – and automated reporting. CISOs are keen on the availability of training, ranking this a long way ahead of other issues.

Smarter tools, more flexibility, and higher headcount would have the biggest positive impact on well-being

As reported earlier, our respondents are now clear on how they measure ROI, with 61.5% saying it comes down to how well they are managing the team in terms of employee satisfaction and retention. Knowing that many cybersecurity leaders are struggling with employee wellbeing and burnout, we wanted to learn what they felt would have the biggest impact on wellbeing and employee retention.

Top of the list was smarter tools that will simplify work (31%), while greater flexibility over working hours and location followed close behind, at the same rate as increasing team headcount (both 28%). This indicates that cybersecurity professionals see technology and human factors as equally important in improving employee experience. The pandemic created new expectations around work flexibility that employees are unwilling to relinquish, while newer industry entrants are digital nomads with high expectations around flexible work. Leaders are also beginning to see the potential of innovations in areas such as AI and low- or no-code to build smarter tools that make work more fulfilling. These are areas that ThreatQuotient will continue to draw on in the future.

REGIONAL VARIATIONS

Once again, we surveyed equal numbers of cybersecurity professionals in the US, UK, and Australia to learn how their experience of cybersecurity automation is changing.

Respondents from the US and Australia are more likely to say cybersecurity automation is important to their company than they were a year ago, with 82.5% and 82% respectively saying it is important. US respondents are the most enthusiastic – 46% say it is very important to their business compared with 26% of Australian respondents who say it is very important. Respondents in the UK continued to become less positive about cybersecurity automation, with the percentage saying it is important having fallen to 61%, a drop from 70% a year ago and 77% two years ago. This fall has been driven by financial services and defense respondents, registering a drop of 28 and 26 percentage points respectively. A fifth (21%) of UK respondents say cybersecurity automation is not important to their organization.

Drivers and use cases for cybersecurity automation vary

The US and Australia see efficiency - how well they use resources such as time, money and skill to get the job done - as the top driver for automation (48% and 39% respectively). In the UK higher productivity - the amount of work that individuals and teams can get through in a given amount of time - is the main benefit sought (36%). This is consistent with last year's findings.

The regions vary on which key use cases they are automating. In the US, the proportion of respondents automating vulnerability management has leapt by 13 percentage points. In the UK and Australia, the dominant use case is phishing analysis, with threat intelligence management in second place in the UK and alert triage taking second spot in Australia. Alert triage also took second place in the US, followed by incident response. In general, US respondents showed a greater likelihood of automating use cases of all kinds.

Every country reported problems implementing cybersecurity automation. The top issue in the UK is "bad decisions" resulting from automated processes - such as blocking domain names that look suspicious but are in fact benign, or blocking an email to the

CEO that turns out to be genuine. This problem was reported by 36% of UK respondents. It was followed by slow user adoption (35.5%) and lack of trust in outcomes (31.5%). For US respondents, their challenges lay in a lack of trust in outcomes (32.5% and a particular problem for US defense respondents), with a lack of skill and bad decisions also causing difficulties. In Australia, lack of trust in outcomes is also the top issue, with Australian financial services the most skeptical in this area. Slow user adoption and a lack of skills are also key barriers for Australian respondents.

Regulatory and compliance challenges are a common problem

In terms of the top three broader challenges facing cybersecurity teams, the main area of agreement was around growing regulatory/compliance requirements, which featured in the top three for all countries. US respondents are most concerned about insufficient budget (26.6%), while high team member churn rate (25.2%) is the number one concern in Australia.

Choosing from a range of statements the one that best matched their organization's current view of cybersecurity automation, US respondents were most likely to say it is "already central to their cybersecurity strategy", while Australian respondents say, "it will become more important as they get better at expanding it". UK respondents are, perhaps unsurprisingly, the most likely to say that "it is causing more problems than it solves".

The global economic picture is affecting budgets in all regions

On the topic of budget, there was very little variation between the countries, demonstrating the global nature of the economic uncertainty we're experiencing. All countries are diverting budget from other areas to bolster automation programs; only around 18.5% were getting net new budget.

The countries agree on the most important feature of cybersecurity automation tools: the ability to integrate multiple data sources. The UK is the only country to feature low total cost of ownership (TCO) in its top three features, perhaps indicating that UK businesses are beginning to work more on optimizing solutions now, as their implementation cycle matures. The availability of training is in the top three for all countries, and US respondents are also looking for visualization tools, while Australian respondents want automated reporting.

Respondents from all regions concur on using how well they are managing the team in terms of satisfaction and retention as the main metric for measuring ROI. The UK is less likely than other regions to be assessing ROI in terms of how well the job is being done (23% use this compared with 33% in the US and 30% in Australia).

In terms of what would make the biggest difference to threat intelligence analyst wellbeing, the regions varied across the three areas of people, process and technology. Australian respondents want more people, UK respondents want more training (process), and US respondents want smarter technology.

ThreatQuotient Take:

The intensifying regulatory/compliance environment, in conjunction with challenging economic conditions, are the two common factors affecting all three countries surveyed. Beyond this, the regions differ on the top use cases and the factors that would make the biggest difference to wellbeing. There is also a decided variation between the UK and other regions on the importance of cybersecurity automation and satisfaction with it, particularly among UK defense and financial services respondents. The reasons for this are not immediately clear and outside the scope of this report, but it will be interesting to see how sentiment changes in the next edition of the study.

VERTICAL SECTOR SNAPSHOT

In general, there has been a rise in the importance that industries place on cybersecurity automation. The only exception is the financial services sector, where the percentage rating it important has dropped from 75% to 69%.

	2022	2023
Central Government	71%	**75%**
Defense	67%	**73%**
Critical National Infrastructure - Energy and Utilities	71%	**82%**
Retail	55%	**77%**
Financial Services	75%	69%

ThreatQuotient Take:

The financial services sector is typically more mature than other sectors on the road to cybersecurity automation, having been an early adopter. As such, it encountered the challenges we have documented over the time we've been conducting this survey at an earlier stage than those in other sectors. Now it is striving to mitigate them and optimize automation deployments. Other industries, earlier in the adoption cycle, are benefiting from advances in automation solutions so may find they have an easier journey.

Industries agree that efficiency is the main driver for adopting cybersecurity automation, but vary on the key use cases

There's consensus across the different sectors on the main driver for adopting more cybersecurity automation: efficiency is the primary goal. The only outlier is critical national infrastructure, where productivity tops the list. But the route to achieving these efficiency and productivity gains varies in terms of the most common use cases for automation in each sector. For central government respondents, the top use case is phishing analysis (35%), while for defense respondents, incident response and threat intelligence management tie at 34%. Critical national infrastructure respondents are most likely to be using it for vulnerability management/prioritization (37%), while in financial services alert triage is the most popular application. In the retail sector it is not surprising that password reset is the top use case (32%).

When analyzing the problems experienced by vertical sector, we find that slow user adoption is the main issue in financial services and critical national infrastructure. However, for defense and retail respondents, the main issue is lack of trust in outcomes. In central government bad decisions and a lack of skill are equally challenging.

The top three challenges for cybersecurity teams vary between verticals

	Central Government	Defense	Critical National Infrastructure	Retail	Financial Services
1	High team member churn rate	Lack of time	High team member churn rate	Growing regulatory/ compliance requirements	Growing regulatory/ compliance requirements
2	Threat environment is escalating faster than our detection/defense capability	Insufficient budget	Lack of time	Alert fatigue (too many alerts for analysts to handle effectively)	Insufficient budget
3	Cybersecurity tool sprawl is causing inefficiencies = Insufficient budget	Growing regulatory/ compliance requirements	Alert fatigue (too many alerts for analysts to handle effectively)	Lack of skills = insufficient budget	Threat environment is escalating faster than our detection/ defense capability

High team member churn rate is particularly troubling in central government and critical national infrastructure organizations, especially given the lengthy vetting processes and industry-specific knowledge required in these sectors. The fact that retail and financial services companies rank regulatory and compliance demands as their biggest challenge reflects the fast-growing swathe of privacy and security regulations that these sectors are subject to.

Financial services and defense organizations are struggling with automation

When looking at how sectors view cybersecurity automation, the financial services story continues to play out. One in five respondents in this sector say cybersecurity automation is creating more problems than it is solving, and those in the defense sector share a similar view. These are both likely to be further in their automation journey and struggling more with challenges and trying to optimize their deployments. Central government respondents are most likely to say it will get more fundamental to their approach as they get better at expanding its use. Critical national infrastructure and retail respondents are positive and planning to roll out more automation in the coming year.

There is strong consensus across sectors on the question of budget, with the majority diverting budget from other teams and tools in order to pursue automation.

In terms of the features they're looking to acquire via cybersecurity automation solutions, the facility to integrate multiple data sources is the top requirement for most. However, for critical national infrastructure respondents the availability of training tops the list, and for financial services low total cost of ownership is the main requirement – again showing how this sector is in the optimization phase of deployment.

Sectors agree that team satisfaction and retention are the best way to measure ROI, but there is variation when considering the best way to make a positive impact on wellbeing:

	Central Government	Defense	Critical National Infrastructure	Retail	Financial Services
Top choice for biggest impact on wellbeing	Investment in smarter tools to simplify work	Greater flexibility over working hours/ location	Consolidation of existing tools to simplify work	Increasing headcount AND more effective cybersecurity automation	More technical training so they become more skilled at using the tools we have

ThreatQuotient Take:

The variations between different vertical sectors suggest that it is important that both vendors and buyers understand where the business is on its cybersecurity automation maturity journey before embarking on the next phase. Conducting a maturity assessment will allow both parties to design more effective solutions that accurately address prevailing challenges and build an achievable roadmap for more successful automation in future. The focus must be on partnership over the long term, rather than attempting "fit and forget" style solutions that can ultimately lead to more pain further down the line. Cyber threats evolve all the time, and so must automation.

ROLE-BASED COMPARISONS

We surveyed various role-holders within the cybersecurity professional cohort, including CISOs, Heads of Cyber Threat Intelligence, Heads of SOC, Heads of Incident Response, Heads of IT Security Solutions Architecture and Managed Security Service Providers (MSSPs). Their different roles put a different lens on their responses. In that vein, while CISOs, Heads of IR, and Heads of CTI are more likely to say the importance of cybersecurity automation has increased, for Heads of SOCs, Heads of IT security solutions architecture and MSSPs, its importance has dropped slightly.

Last year, we found a disconnect between different role holders across several questions, and this year those variations continue. For instance, while increasing efficiency is the top driver for introducing automation for CISOs by some margin (42%), for Heads of SOC and MSSPs regulation and compliance is the top driver.

Automation use cases and wider team challenges vary between roles

Alert triage is the top use case for CISOs, but among Heads of SOC it is threat hunting, pointing to their focus on proactive defense. And, unsurprisingly, Heads of IR are keen on automating both incident response and vulnerability management.

For CISOs, bad decisions are the most common problem affecting their automation program (40%), while lack of skill affects Heads of SOC the most (36%). For Heads of CTI it is lack of trust in outcomes (33%), perhaps indicating that analysts feel human oversight is preferable to machine-driven analysis. Heads of IR and Heads of IT security solutions concur that there is a lack of trust in outcomes, while for MSSPs slow user adoption is the main issue.

In terms of wider challenges facing cybersecurity teams, CISOs report concerns across the board. High team member churn rate is their most pressing issue (25%) (and they are also the most likely to say increasing headcount would make the biggest impact on wellbeing). High team churn rate is the second most common problem cited by Heads of SOC, although it comes after insufficient budget and lack of training on key tools, which are joint top for this group.

Heads of IR say tools sprawl is causing inefficiencies – it's their joint largest challenge alongside regulatory/compliance requirements. Heads of IT solutions architecture are challenged by a lack of time, while for MSSPs it is regulatory/compliance requirements. Again, the lack of consensus among roles over the challenges they face (particularly between CISOs and the roles that report to them), points to a disconnection on priorities and direction.

Views on cybersecurity automation differ

The majority view among CISOs is that cybersecurity automation will become more important as they get better at implementing it (21%), although a solid 15% say it is

causing more problems than it solves. Heads of SOC mainly say it is already central to their cybersecurity strategy (22%), although again 16% say it's causing problems. Heads of Incident Response predominantly say that they are planning greater cybersecurity automation adoption in the coming year (24%), while Heads of IT Security Solutions/ Architecture are split, but 18% say momentum behind it has stalled. MSSPs seem to be having a particularly challenging time, with 23% saying cybersecurity automation has caused more problems than it solves.

In terms of top features sought from cybersecurity automation tools, the roles have differing priorities:

Top feature sought	Role
Availability of training (27%)	CISO
Visualization tools (28%)	Head of SOC
Facility to integrate with multiple data sources (26%)	Head of CTI
Facility to integrate with multiple data sources (25%) AND Vendor Support (25%)	Head of IR
Automated reporting tools (23%)	Head of IT Security Solutions Architecture
Tools that support cross-team collaboration (30%)	MSSPs

Roles agree on how to measure ROI, but not on how to boost analyst wellbeing

There is a general consensus on how to assess ROI – by how well the team is being managed. However, there is disagreement over what will make the biggest positive impact on threat intelligence analyst wellbeing. Overall, investment in smarter tools is seen as having the biggest impact, but CISOs feel that increasing headcount would make the most difference, followed by more flexible working. Investment in smarter tools is only third on their list.

ThreatQuotient Take:

Better analyst wellbeing is a win on many fronts. It should lead to greater employee retention, helping organizations avoid high recruitment costs in a challenging employment market. It also lowers the risk of losing valuable corporate knowledge when key team members leave. However, it appears that a multi-faceted approach is needed to address wellbeing, including investment in smart tools, the provision of training and support, and offering a flexible working environment. Businesses should not feel that they have to do all this alone, but should create partnerships with vendors to ensure the solutions they invest in are supported throughout implementation and adoption. This should include training that gives analysts confidence in the tools at their disposal and helps overcome the adoption hurdles that are holding cybersecurity automation back.

THREATQUOTIENT RECOMMENDATIONS:

As we consider the latest research findings on cybersecurity automation in 2023, it's clear that progress has been made over the past year. Organizations have been actively using automation to streamline routine tasks and improve their cybersecurity posture. However, even with this progress, significant challenges remain. Complex technological landscapes, skill shortages, and difficulties in securing management support remain as roadblocks. This section of the report distills the insights from the research into five actionable recommendations tailored for security professionals responsible for automation efforts. These recommendations serve as guidelines for enhancing the effectiveness and efficiency of cybersecurity automation initiatives.

1. **Invest in Smart Tools and Flexibility for Wellbeing:** To improve threat intelligence analyst wellbeing and employee retention, invest in smarter tools that simplify work processes. Smart tools equipped with AI capabilities empower analysts to make faster and more accurate decisions. Additionally, offer greater flexibility in working hours and locations, enabling employees to maintain a healthier work-life balance. These enhancements can contribute to a more positive work environment and increased job satisfaction.
2. **Choose Proven Use Cases for Automation:** Select cybersecurity automation use cases that have demonstrated value by saving time and improving security procedures. Popular choices, such as threat intelligence management, incident response, phishing analysis, and vulnerability management, offer tangible benefits in terms of efficiency and effectiveness. These use cases provide a solid foundation for building a successful automation strategy.
3. **Integrate Data Sources for Contextual Insights:** Emphasize the importance of integration with multiple data sources when selecting cybersecurity automation solutions. This integration enhances context for decision-making, enabling automation to focus on relevant and high-priority events. Data-driven automation ensures that actions are aligned with the real-time threat landscape and continuous improvement is driven by accurate insights.
4. **Address Implementation Challenges through Training:** Recognize that implementing cybersecurity automation is not without challenges. Combat issues like "lack of trust in outcomes" and "slow user adoption" by investing in comprehensive training programs. Training not only equips your team to use automation tools effectively but also boosts user confidence, mitigating issues related to implementation hurdles.
5. **Align Automation Metrics with Organizational Goals:** Secure management support for automation initiatives by defining clear metrics for success and aligning them with organizational goals. Balance quantitative metrics, such as improved efficiency and resource management, with qualitative factors like employee satisfaction and retention. Demonstrating a broad impact encourages ongoing support and investment in automation.

By following these recommendations, organizations can navigate the complexities of cybersecurity automation adoption, harness its potential benefits, and effectively address challenges to enhance overall security posture and operational efficiency.

QUESTION RESPONSES:

How important is cybersecurity automation to your organization?

The percentage of cybersecurity professionals saying that automation is important to their organizations has risen significantly compared to 2022. Three quarters (75%) now say it is important, up from 68% last year. Almost one third (32%) say it is very important while a further 43% say it is somewhat important.

Only 12% say cybersecurity automation is not important to their company.

Mirroring last year's trends, the larger an organization is, the less likely they are to place importance on cybersecurity automation.

What, if any, are the main drivers behind your organization's need to adopt more cybersecurity automation?

Increasing efficiency is a top priority for most respondents, with 41% choosing it. This is followed by regulation and compliance (38%) and increasing productivity (36.5%). Interestingly, maintaining cybersecurity standards has dropped down the priority list from a first place tie last year, to fifth this year. This may reflect greater pressure on efficiency and productivity measures as the economic situation has become more challenging over the last year, rather than a loss of interest in performance. Just over one third see addressing the skills shortage as a key driver for automation.

ThreatQuotient Take:

It is interesting that regulation and compliance are driving automation adoption. There is no doubt that regulators are paying increasingly close attention to the cyber strategies that organizations have in place to protect data and prevent breaches. It may be that cybersecurity professionals see automation can help in compliance work where there are a lot of repetitive exercises.

What, if any, cybersecurity processes/use cases do you automate today in your organization?

	2022	2023
Phishing analysis	26%	**31%**
Incident response	26.5%	**30%**
Vulnerability management/prioritization	25%	**30%**
Alert triage	18%	**30%**
Threat intelligence management	26.5%	**29%**
Password reset	21%	**28%**
Threat hunting	25%	**27%**

Compared to last year, companies are automating more processes in general. For example, the percentage automating alert triage jumped from 18% to 30%, indicating that this use case in particular is taking off.

Incident response and phishing analysis remain popular use cases for automation and vulnerability management has risen up the list compared to last year.

ThreatQuotient Take:

Incident response is a great place to leverage automation, due to its multi-stage, multi-tool process. When handled manually it is classically slow – the incident takes place, a ticket is created, and the team manually collates evidence to see what the incident might be. It entails using a lot of different tools with data that is manually collated before any conclusion can be attempted. By using automation to collate and contextualize the data emanating from multiple sources, response times can be considerably accelerated, and the amount of admin analysts need to do is reduced.

Has your organization encountered problems/issues when implementing cybersecurity automation, and if so, what problems/issues have arisen?

The result is unanimous: implementing cybersecurity automation is never problem-free. 100% of respondents have experienced some sort of issue. When we relate this to the drop in perception of the importance of automation in some segments of the research cohort, we can see here the areas that are causing them problems.

The main problem – which appeared to have receded last year but was prominent in 2021 - has shot back to the forefront once again: “lack of trust in outcomes” is cited by 31%. Close behind is slow user adoption (30%) and it isn’t hard to see how these two are linked, especially in an environment where there is high team member churn, which also leads to low user adoption as personnel rotate.

“Bad decisions” comes in third position (29%) and lack of skill is fourth (28%). Interestingly management buy-in/understanding has dropped significantly; last year it was the most common problem, but now it is the least.

ThreatQuotient Take:

This could signify that management has now got behind the idea of cybersecurity automation and signed off on projects, but now those projects are coming to implementation and the problems are emerging. Certainly, it seems that businesses are not finding it as easy as they might have hoped to implement automation solutions. The introduction of low and no-code solutions may ease this tension, and organizations should also consider the value of training to support employees to make better use of tools Indeed, 23% of respondents (rising to 27% of CISOs) say that the availability of training is an important feature when they are selecting automation solutions.

What are the biggest challenges your cybersecurity team currently faces?

Too little money and too many regulations are challenging cybersecurity teams, as "insufficient budget" and "growing regulatory/compliance requirements" top the list, affecting 24% in each case.

Not far behind is the high team member churn rate (23%). The rapidly escalating threat environment moving faster than detection/defense capability is affecting 23%, as is lack of time (23%).

21% said that cybersecurity tool sprawl is causing inefficiencies, and the same number noted a lack of skills and alert fatigue. 17% said there was a lack of training on key tools.

Larger organizations appear to be less troubled by team churn, but they are more likely to be challenged by growing regulatory issues and a lack of time. They are also more likely to say their teams need training.

ThreatQuotient Take:

It is clear that cybersecurity teams are facing challenges on several fronts. Intelligently applied cybersecurity automation can help organizations address budgetary challenges - partly because it helps preserve license capacity among the tools that are integrated into the platform - and also by helping analysts become more efficient and productive. On a similar theme, automating repetitive tasks can help keep analysts engaged and focused on higher-value activities, reducing the likelihood that they will be tempted to look elsewhere for a more fulfilling role.

What is the predominant view of cybersecurity automation in your organization right now, if any?

Overall, respondents are divided about cybersecurity automation. 19% say "it will become more important as they get better at expanding it", and 18.6% are "planning more cybersecurity automation adoption in the coming year". For 17% it is already "central to their cybersecurity strategy, putting them ahead of their adversaries".

Nevertheless, 16% say it is "causing more problems than it solves", 14% say "momentum has stalled", and 14% "would like to use more but are struggling to do so".

More than one in five (22%) of organizations over 10,000 employees say that cybersecurity is central to their strategy and puts them ahead of adversaries, which is a notably higher rate than for smaller organizations. At the other end of the scale, respondents from financial services and defense organizations are more likely to say it is causing more problems than it solves, with 21% and 18% saying this respectively.

In terms of the roles, it is Heads of SOC that are most likely to say cybersecurity automation is already central to their strategy (22%), which may be down to the fact that automation solutions were initially designed with the SOC in mind. Heads of IR are most likely to say they are planning to introduce more automation in the coming year (24%), perhaps evidence of further momentum uncovered in the response to question 3.

ThreatQuotient Take:

The diversity of views - some positive, some negative - expressed by respondents demonstrates the evolving nature of the cybersecurity automation adoption. The first generation, process-driven solutions implemented by early adopters have revealed some shortcomings, but now low/no-code data-driven platforms are addressing many of the problems encountered. This should lead to better experiences for the next wave of cybersecurity automation adopters; it will be interesting to see whether this indeed proves to be the case.

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

Budgets are rising again, but funds are coming from different directions compared to last year. All but one respondent reported their budget for cybersecurity automation has increased for one reason or another. The most common approach was allocating budget from outside the security team (57%), while 46% had increased it through allocating budget from other tools (e.g. SIEM), and 27% had allocated unused headcount budget. This is a slight drop on last year, when 32% had done this.

Only 18.5% report that they have a net new budget to use, a drop on the 34% that said this last year. This rises to 21% in the UK and drops to 16% in Australia. The only role getting more net new budget is managed security service providers, which is not surprising as – when your core business is security – it is essential that you invest in it. It becomes a product and service offering, rather than a risk management exercise.

There is a very strong consensus across industries and vertical sectors on the budget question. It is clear that the prevailing economic conditions are having an impact. While organizations are choosing to invest in cybersecurity automation, they are having to make some hard choices about where to trim other budgets to do so.

ThreatQuotient Take:

Despite its challenges, cybersecurity automation is clearly viewed as a priority area and a focus of investment - even when this means reprioritizing funds from other areas. It is here to stay as a core element of cybersecurity strategy so now the emphasis must lie in resolving those challenges and ensuring it works well and delivers on business objectives.

What are the most important features when you are selecting cybersecurity automation solutions?

Integration with multiple data sources (24%), training availability (23%), and automated reporting tools (21%) top the wish list for organizations when choosing cybersecurity automation solutions.

This is followed by visualization tools (21%), and tools that support cross-team collaboration (20.5%).

Lower down the list are "a clear route to achieving ROI", alert prioritization, low TCO and the facility to integrate with existing cybersecurity tools (all 19%).

ThreatQuotient Take:

There are undoubtedly themes emerging here that relate to findings from the wider research. It's important that tools integrate multiple sources, but also important that teams know how to use them, and that adoption is supported to avoid team churn and make work more satisfactory.

What, if any, are the metrics you use to measure cybersecurity automation ROI/KPIs?

Views have crystallized on how best to measure ROI/KPIs for cybersecurity automation. 61.5% say it is about how well they are managing the team (employee satisfaction/ retention) – up from 39% that said this last year. This aligns strongly with the fact that team churn is a key challenge for many organizations and vertical sectors.

One third said they used how well they are managing resources such as staffing, efficiency/effectiveness and budget as a key metric. 29% said it was how well they are managing to do the job.

There was broad consensus across job roles and sectors indicating that, in the difficult climate we're experiencing, businesses really want to keep their teams.

What would make the biggest positive impact on threat intelligence analyst wellbeing and employee retention in your organization?

People and technology sit at the heart of improving cybersecurity analyst wellbeing. Investment in smarter tools to simplify work (31%) is the top response, reflecting respondents' view that smart tools can significantly enhance the experience of work for their employees. More directly, greater flexibility over working hours/location (28%) and increasing team headcount (28%) make up the top three factors. Several other factors are almost as highly rated, including more technical training, more effective cybersecurity automation (both 27%), and more wellbeing training (26%).

ThreatQuotient Take:

The introduction of AI into cybersecurity automation platforms will make smart tools even smarter in the near future. Used carefully within the cybersecurity threat intelligence environment, AI can empower analysts to make better decisions, faster, armed with the right context and evidence they need to prioritize threats and vulnerabilities and respond effectively.

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**.

TQ-RPT01-1123-03