

Evolution

THE ~~STATE~~ OF
CYBERSECURITY
AUTOMATION
ADOPTION

AT-A-GLANCE



On Cybersecurity Automation...

Growing in Importance: 80% of respondents say cybersecurity automation is important to their organization. This percentage has risen every year since 2022.

Top Use Cases: Incident response, Threat hunting, and Phishing analysis are persistently popular use cases for automation. These are the use cases organizations should explore first as they have proven their value.

Trust in Automation is Improving: Just 20% of respondents say they don't trust the outcomes of automated cybersecurity processes in 2024, a drop from 31% last year .

Budget Allocation: 99% have more budget for cybersecurity automation. This year, many more organizations (39%) have net new budget, indicating the proven value of cybersecurity automation in business cases.

Measuring Success: Team wellbeing remains the top automation KPI. It's automation's impact on employees that matters, ahead of performance and efficiency metrics, although these are rising in prominence compared to last year.

On Cybersecurity Strategies and the Threat Environment...

Threat Intelligence Sharing for Internal and External Collaboration: 99% share threat intelligence through at least one channel. 54% share with direct partners and suppliers and 48% through an official threat-sharing community.

Integration is Key: The ability of cybersecurity tools to integrate with others is critical. 67% use some form of integration within their tool stack.

AI as a Scale Function: 58% are using AI in their cybersecurity strategy. 29% are using it across all operations and 29% in specific use cases.

2025 Attack Landscape: Cyber-physical attacks are the most commonly expected attack type in the coming year. Phishing, ransomware and malware are close behind.

Dive into the report to see the how these statistics vary in different countries, vertical sectors and senior cybersecurity roles.

KEY FINDINGS

47%

Measure cybersecurity automation ROI on the basis of employee satisfaction/retention

COMMON CYBERSECURITY AUTOMATION CHALLENGES



Technology issues



Lack of budget



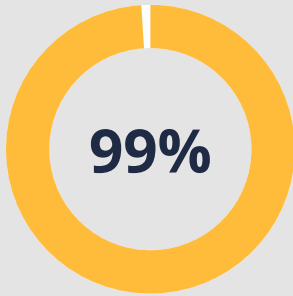
Lack of time

TOP USE CASES FOR CYBERSECURITY AUTOMATION:

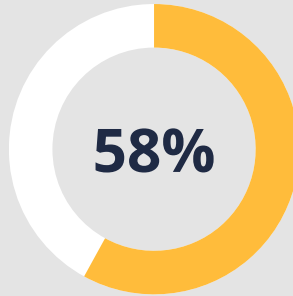
- 1 Incident Response
- 2 Phishing Analysis
- 3 Threat Hunting

EXPECTED ATTACK VECTORS IN THE YEAR AHEAD

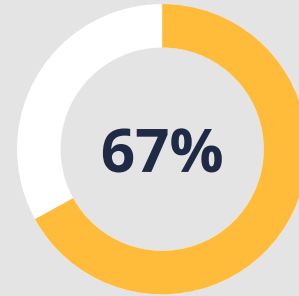
- 1 Cyber-physical attacks
- 2 Phishing
- 3 Ransomware



Have increased budget to invest in cybersecurity automation. Among these 39% have net new budget



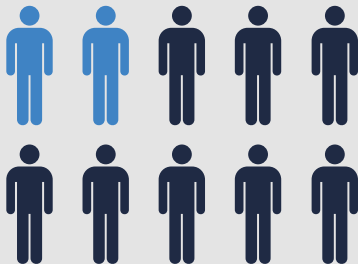
Are using AI in cybersecurity



Integrate third-party solutions into their security architecture

80%

Say cybersecurity automation is important to their organization



99%

Share cyberthreat intelligence in some form with other parties

TABLE OF CONTENTS



At-A-Glance	2
Key Findings	3
Table of Contents	4
Foreword	5
Research Insights	8
Regional Variations	16
Vertical Sector Snapshot	20
Recommendations	29
About the Report & Methodology	30

FOREWORD

Welcome to the new normal: cybersecurity automation for resilience and scale

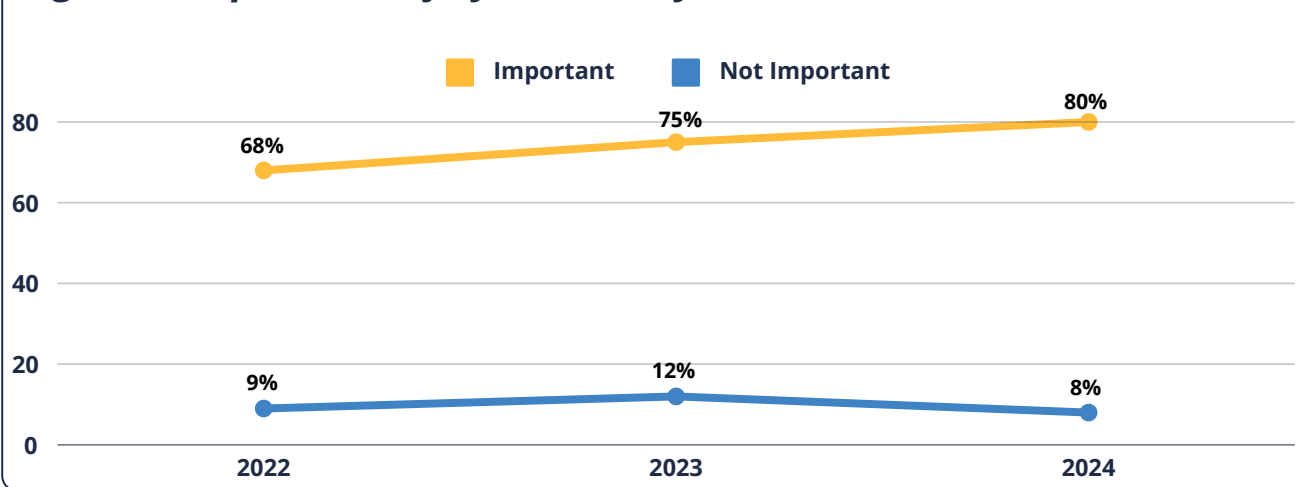
During the period from 2020-2024 in which we have conducted our annual study into the State of Cybersecurity Automation the world has experienced continuous disruptive change. From the pandemic and rising geo-political tension to the global energy crisis, economic downturn, and challenges to national elections, the list is long and diverse. These issues have been echoed, amplified, scaled, and intensified throughout the cyberthreat environment. Cybersecurity professionals now face fast-changing cyber and cyber-physical threats of unprecedented sophistication, volume, velocity, and variety.

But cybersecurity professionals have not become paralyzed by the enormous task of defending their business. Resilience is now the byword for effective cybersecurity in recognition that successful organizations are those with the people, processes, and technology in place to respond to whatever threat comes, wherever it comes from. In this new normal of continuous rapid change, organizations are now focused on taking seismic events in their stride without compromising their business objectives.

At the same time, cybersecurity professionals have grown more experienced, their skills have developed, and they have adapted to a volatile and unpredictable reality. During that process, they have adopted cybersecurity automation as an important part of their defensive strategy (Figure 1). Now, they want targeted, customized automation, allowing them to pivot people and resources to where they're needed.

The regulatory landscape has shifted too, as authorities seek to build resilience at industry and cross-border scale. The second Network and Information Security Directive (NIS2) and Digital Operational Resilience Act (DORA) are just two among several regulations seeking to improve cybersecurity standards and promote collaboration. This adds a compliance lens to the challenge of robust cyber defense.

Figure 1: Importance of Cybersecurity Automation (%)





Hype versus reality

The path to cybersecurity automation adoption has not been straightforward. It has largely followed the [“hype cycle”](#) of emerging technologies devised by Gartner to help organizations make decisions about technology adoption. Our research has tracked organizations through a cycle of enthusiasm and high expectations, followed by difficulties and disappointment, before landing on several specific use cases that work for their organization. Cybersecurity automation has also progressed from being a standalone objective to becoming an integral feature within many tools. As such, it now shows strong signs of crossing the chasm towards the “plateau of productivity” as value is found in various use cases and solutions, and trust in outcomes rises.

Consequently, after a period where external economic and societal factors have dominated decision-making, organizations are now focusing on what matters to them across their own industry and particular role. They are becoming more micro-focused versus macro-driven, which is where the value of automation can be found, enabling teams to respond to the specific threats and challenges facing their business.

Budget for cybersecurity automation has increased every year, but this year’s survey finds more net new budget being allocated to investment in cybersecurity automation. Previously, decision-makers were diverting budget from other cybersecurity tools or reallocating unused headcount funds. In 2024, more now have a business case for dedicated budget, another indication that cybersecurity automation is maturing.

People, process, technology: cybersecurity automation cements the virtuous circle

Organizations continue to view employee satisfaction and retention as a key measure of cybersecurity automation return on investment (ROI) and value; it’s a significant KPI for 47%. Cybersecurity automation is one of the clearest applications of the “people, process, technology” mantra for success. By automating the right processes in each use case and integrating the right technology, organizations can deliver positive outcomes for the people they employ, and that’s the rationale behind employee satisfaction as a key metric.

On a related process and technology note, this year’s survey dived deeper into how organizations approach the cybersecurity technology stack. It underlined the importance of seamless integration of different cybersecurity solutions and the data they generate. Just under half of survey respondents (45%) opt for a best-of-breed approach, integrating different solutions together to achieve an optimum environment. However, even among the 55% of organizations that prefer a single vendor approach, 35% still integrate third-party solutions where necessary, emphasising the added value in tools that can work together seamlessly.



Automation and AI are scale functions for cybersecurity teams

As businesses adapt to this new normal of rapid change and high volume, diverse attacks, scaling cybersecurity is the next big challenge. Cybersecurity automation is central to this, and while earlier surveys revealed a lack of trust in automation outcomes, this edition shows greater confidence.

Looking ahead, Artificial Intelligence (AI) offers similar benefits of scale, and our survey found that 58% of organizations are already using it in cybersecurity to some extent. However, we anticipate that AI in cybersecurity – currently sitting at the “peak of inflated expectations” – will pass through the same adoption cycle and challenges experienced by automation, including trust issues and technical deployment issues, before it is applied to the right use cases and becomes truly productive.

In this year’s research, we also looked at how organizations are approaching threat intelligence sharing. It is a critical element of a collaborative approach to cybersecurity and features heavily in upcoming regulations such as DORA, NIS2, and SEC cybersecurity disclosure requirements, as authorities seek to elevate cybersecurity performance, gain an accurate picture of risk, and tip the balance in defenders’ favor. Sharing threat intelligence is also a key use case for automation; it helps organizations and industries scale knowledge exchange and fuel collaboration.

Finally, we looked at the threats organizations expect to face most often in the coming year. This is an area where respondents keep a keen eye on macro influences such as geopolitical and social unrest, with cyber-physical attacks topping the list ahead of phishing, ransomware, and malware.

Based on the research results, ThreatQuotient believes that scaling security operations and collaboration across teams, ecosystems, and industries is the most urgent challenge facing cybersecurity professionals. Successfully uniting human expertise, automation, and AI, and enabling seamless integration across tools and intelligence feeds will drive greater cyber resilience and agility at organizational, industry, and international levels. Everyone’s new normal is different, and maturity levels vary between industries, but by focusing on the use cases that deliver value and sharing intelligence, we can create a rising tide effect, resulting in more effective, proactive cyber defense.

We hope you find this report interesting and valuable.

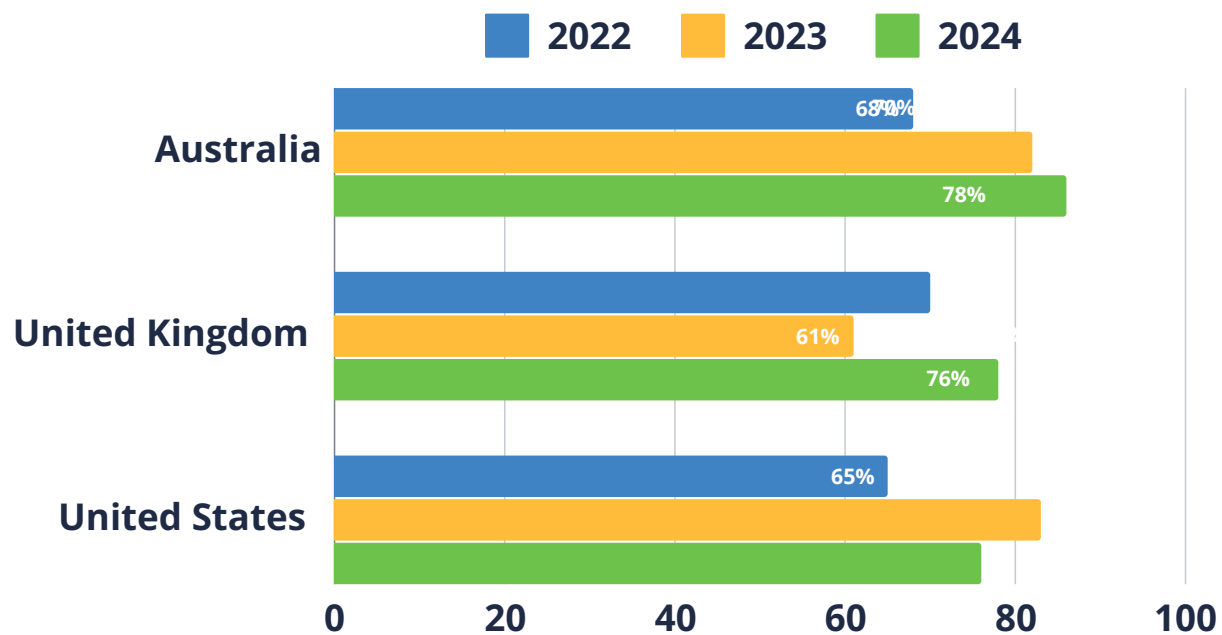
As businesses adapt to this new normal of rapid change and high volume, diverse attacks, scaling cybersecurity is the next big challenge.

RESEARCH INSIGHTS



The importance of cybersecurity automation has risen significantly in the new normal of constant change

Figure 2: Importance of Cybersecurity Automation (%)



Eight in ten respondents now say that cybersecurity automation is important to their organization; just over one-third say it is “very important” (Figure 2). In the UK, the percentage rating cybersecurity automation as important has jumped from 61% in 2023 to 78% this year. Conversely, US respondents are less positive, with a drop from 82.5% rating it important last year, to 76% this year. This may indicate that some US respondents are entering a period of disillusionment with cybersecurity automation, similar to that experienced in the UK in 2023.

Only 6% say cybersecurity automation is not important to their organization, down from 12% in 2023.

Efficiency and productivity remain the top two drivers for adopting cybersecurity automation overall,

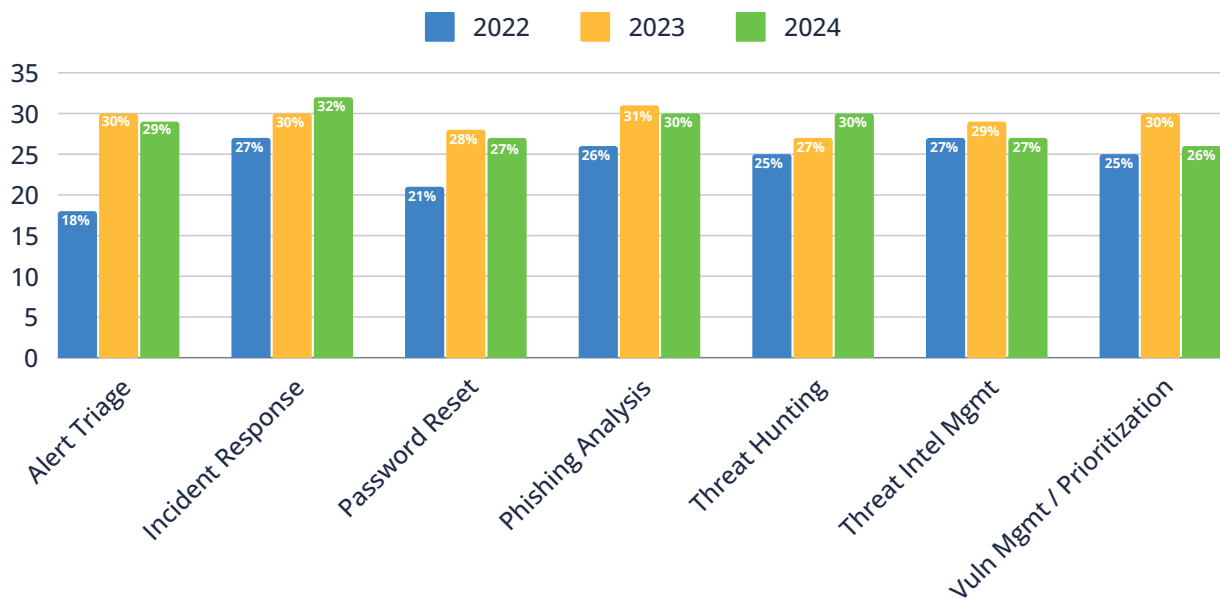
although in the defense and critical national infrastructure sectors improving cybersecurity standards is viewed as a more important driver. These sectors are also the most likely to cite cyber-physical attacks as the most common attack vector expected in the coming year; this disruptive threat for these key verticals may be behind their drive to raise security standards.

The survey finds a strong correlation between organizations that view cybersecurity as important and those that are already using AI in cybersecurity. Ninety-two percent of those using AI everywhere in cybersecurity say automation is important, compared to just 66% of those that have not yet deployed AI.

Organizations identify key use cases as automation crosses the chasm to productivity and trust in outcomes rises

Incident response is the most popular use case for automation, rising consistently through the course of the study (Figure 3). The use of automation in threat hunting has also continued to rise, while phishing analysis, threat intelligence management, and password reset have held steady as popular use cases. Organizations seem less certain about automation for vulnerability management, recording a drop compared to last year.

Figure 3: Automation Use Cases (%)

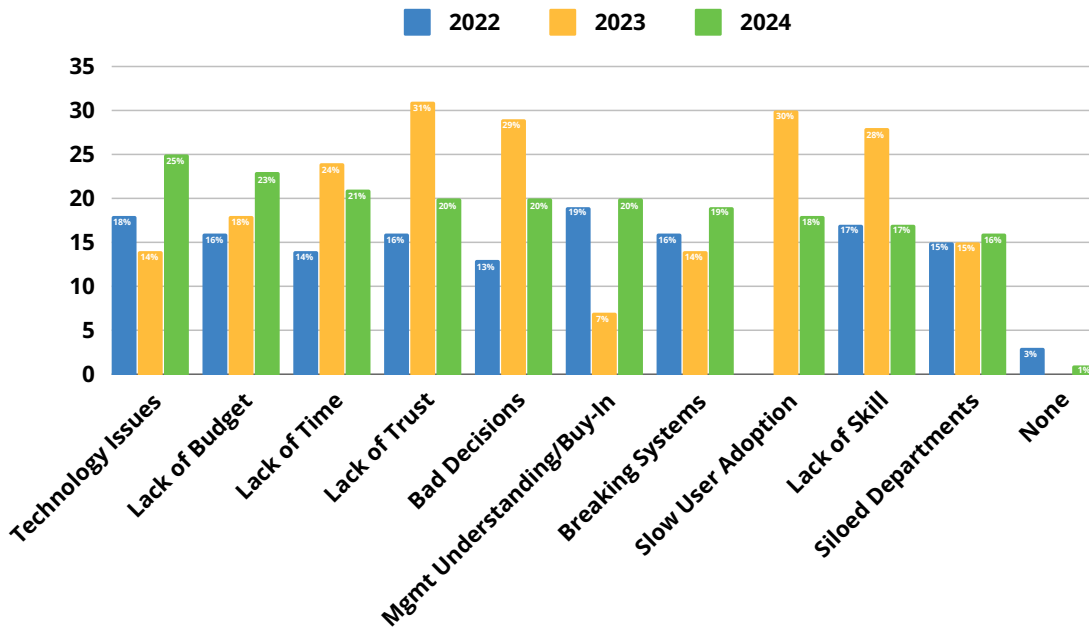


ThreatQuotient Take:

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 work admin analysts need to do is significantly reduced.

As automation deployments mature, trust in the outcomes of automated processes has increased (Figure 4). Just 20% of respondents now report lack of trust as a key challenge to implementation, a drop from 31% last year. In 2023, there was significant concern around trust, bad decisions, slow user adoption, and lack of skill, but these concerns have abated in 2024.

Figure 4: Problems When Implementing Cybersecurity Automation (%)

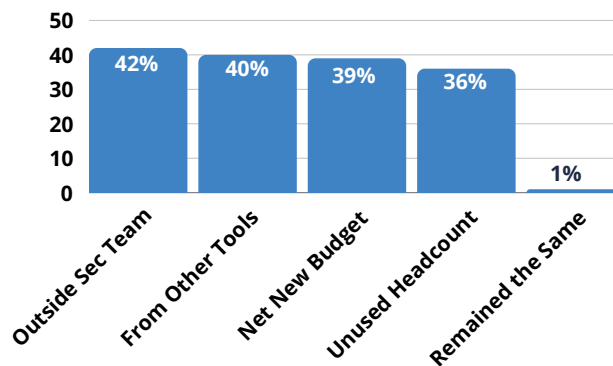


Automation budget increases

Budget for automation has risen in every year we have conducted our study. This year 99% of respondents say they have more budget. However, the way they are sourcing cybersecurity automation budget has changed. Thirty-nine percent now have net new budget specifically for automation (Figure 5), a rise on just 18.5% last year.

Better understanding of key use cases and the benefits automation is delivering as deployments mature is helping organizations make stronger business cases to secure budget.

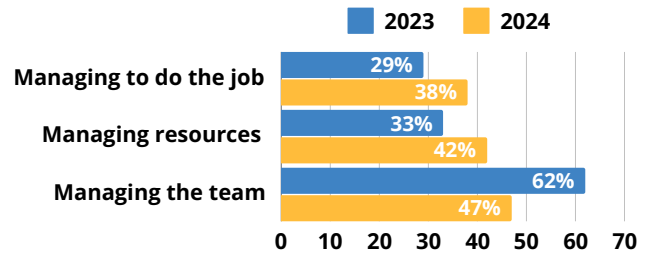
Figure 5: Automation Budget Increases (%)



Team well-being and employee retention still lead KPIs, but resource efficiency and performance are growing in importance

“Managing the team, as reflected by employee satisfaction and retention” remains the top metric for assessing ROI (Figure 6). However, while 61.5% cited it as the key metric in 2023, fewer (47%) do so in 2024. Resource management, in terms of staff efficiency, effectiveness, and budget, and how well the job is being done in terms of MTTR and MTTD have both become more prevalent as measurement tools.

Figure 6: Measuring KPIs (%)



CISOs are more likely than respondents in other roles to rank employee satisfaction and retention as the main ROI metric of importance, reflecting the people management focus of their role. It also remains the lead metric by some distance for respondents in the defense sector, where employee churn can cause problems as security clearance for new employees adds to the recruitment burden.

ThreatQuotient Take:

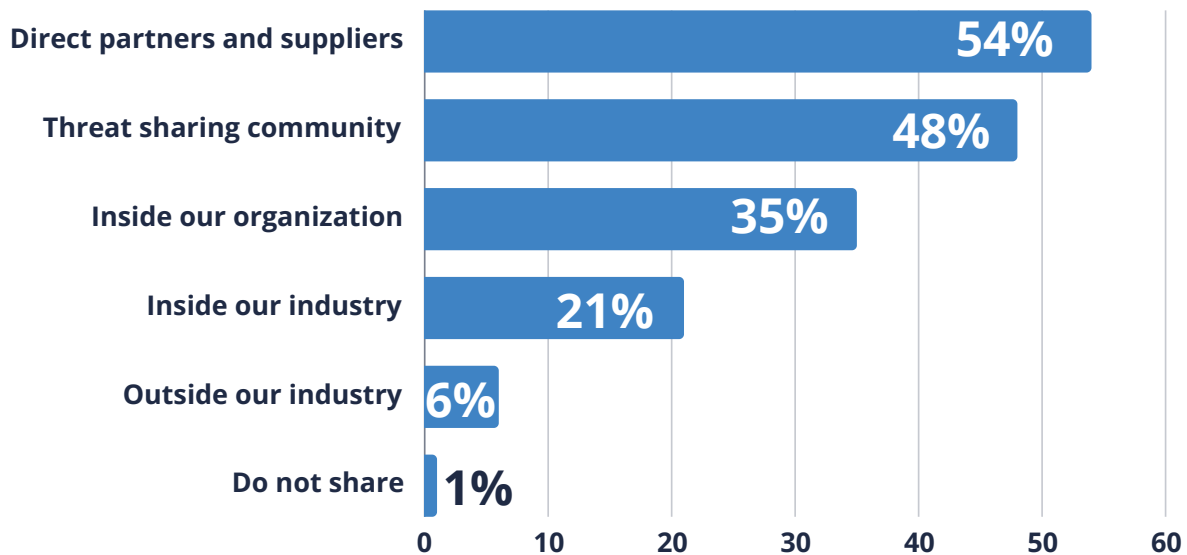
As organizations grow more focused on the micro-environment, they are homing in on metrics more closely linked to productivity and efficiency. The post-pandemic-influenced wellbeing focus is waning and, while employee retention and satisfaction remains important, it is no longer heavily outweighing performance and efficiency metrics.

Threat intelligence sharing has momentum: 99% share through at least one channel

Ninety-nine percent of cybersecurity professionals surveyed say they share cyber threat intelligence through at least one channel. Sharing with direct partners and suppliers is the most popular activity, undertaken by more than half of respondents (54%) (Figure 7), which may reflect recent regulatory changes making organizations responsible for vulnerabilities in their supply chain.

Sharing within industries is also fairly common, through both official channels such as Information Sharing and Analysis Centers (ISACs) and unofficial channels, but organizations are less likely to be sharing outside their industry.

Figure 7: CTI Sharing Approach (%)



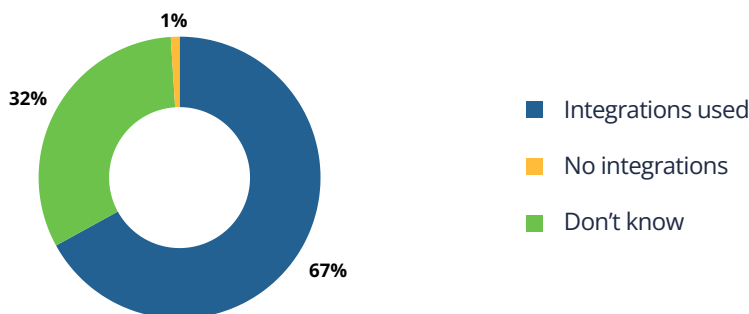
ThreatQuotient Take:

Intelligence-sharing is a great use case for automation, allowing companies to share their own intelligence with third parties. We anticipate that threat intelligence sharing will continue to mature and scale as regulatory requirements come into force and the need to develop associated best practices exerts influence on organizations. Businesses should factor in the ease and efficiency with which their threat intelligence solutions enable them to collaborate both within and beyond their organization.

Integration is key as organizations take a diverse approach to cybersecurity technology

Two thirds of respondents integrate best-of-breed solutions into their security architecture, regardless of whether they focus solely on best-of-breed solutions or start with a single-vendor platform which they supplement with best-of-breed tools where necessary. This underlines the importance of vendors ensuring that their solutions can integrate with others and share data seamlessly. (Figure 8)

Figure 8: Approach to Selecting CTI Tools (%)



ThreatQuotient Take:

This finding chimes with our experience. Typically, our customers have around 34 tools delivering data that they need to integrate into other solutions in order to get full visibility and control over their environment. That's why the ThreatQ Platform supports a huge ecosystem of over 450 products and feeds, enabling customers to get maximum value out of their cybersecurity investment.

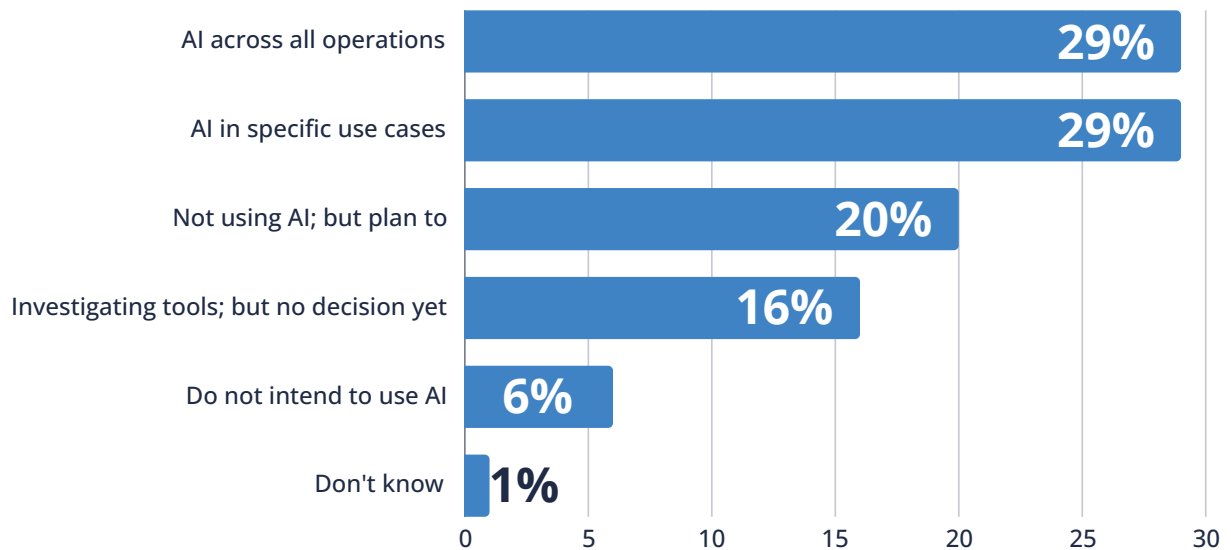
AI adoption gathers momentum – potentially driven by platform providers

Fifty-eight percent of respondents say they are using AI in cybersecurity (Figure 9). Half are using it everywhere, and half in specific use cases. A further 20% are planning deployments.

There is evidence that an organization’s approach to technology is influencing how it approaches AI adoption, too, with a strong correlation between respondents who are using a single vendor platform as the foundation to their security architecture and AI deployment. Sixty-two percent of organizations that use a standalone single vendor platform say they are using AI across all operations, indicating that their platform provider has introduced AI.

In contrast, respondents using best-of-breed solutions that don’t integrate together are further behind in adoption – just 22% use AI in any form. Organizations that prefer a best-of-breed approach with solutions working together are more likely than average to be using AI in specific use cases (42%). Again, this is likely because individual solution vendors are introducing AI capabilities.

Figure 9: The Use of AI in Cybersecurity (%)



ThreatQuotient Take:

As AI rollout accelerates, organizations need to stay alert to its introduction by platform providers and solution vendors and check that they are comfortable with the use cases it's being applied to, and also that they are getting the most benefit from AI implementation. A word of caution, too: AI is a nascent technology with varying interpretations and definitions, which makes it difficult to make confident statements on market adoption. It is reminiscent of the early days of cloud adoption – everyone says they are doing it but what they are doing is not the same in every case.

Cyber-physical attacks considered most likely in the coming year

Cybersecurity professionals expect cyber-physical attacks, phishing, ransomware, and malware to dominate in the next 12 months. The rise in profile of cyber-physical attacks reflects their disruptive potential as physical systems, transport networks, and buildings increasingly depend on digital management systems. Accordingly, defense and critical national infrastructure respondents are most concerned about this type of attack. Financial services organizations are more concerned than average about ransomware, while central government respondents are most concerned about state-sponsored attacks.

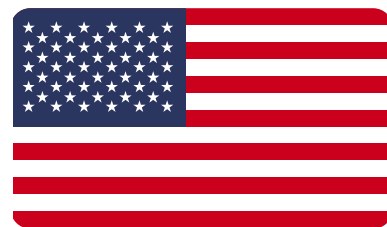
Although not a top-three vector, attacks via the supply chain are expected by 22% of respondents, and one in five expect to see state-sponsored attacks affecting their business.

Expected attack types vary across geographies

	AUS	UK	US
1	Cyber-physical attacks	Malware / Phishing	Cyber-physical attacks / Phishing
2	AI-powered attacks	Cyber-physical attacks	Denial of service attacks
3	Deep fakes / supply chain / malware	Ransomware / Denial of service	Attacks via supply chain

ThreatQuotient Take:

Respondents demonstrate a broad spread of concerns about a diverse range of attack vectors. This reflects the new normal, where cybersecurity professionals are focusing closely on the threats that are likely to have the highest impact on their specific industry, role, and region in a bid to build resilience and adaptability. It emphasizes both the scale and breadth of focus that defenders need to devote to their work. It also underlines the importance of cyber threat intelligence that's tuned for the threats specific to each organization and industry.



REGIONAL VARIATIONS

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

This year, UK respondents are far more positive about cybersecurity automation than they were in 2023. Seventy-eight percent say it is important to their organization and 32% say it is very important. This is an encouraging bounce back from last year where only 61% said it was important. US respondents are less positive; they are perhaps experiencing a cyclical period of frustration with automation aligning with Gartner's "trough of disillusionment" phase. Seventy-six percent now say it is important to their company, compared to 83% last year. The US dip is influenced by respondents from central government organizations, where only 60% attach any importance to cybersecurity automation.

In contrast, Australian respondents remain very positive, with 86% now rating cybersecurity automation as important, up from 82% in 2023.

ThreatQuotient Take:

This US pessimism may also result from general economic and political uncertainty in the region at the time the research was conducted; in our experience, higher level issues like this often influence cybersecurity sentiment and negatively impact confidence.



Use of AI in cybersecurity varies geographically and correlates with technology approach


Australian respondents are most likely to say they are using AI across all cybersecurity operations, with 44% saying they are doing so, compared to 30% in the UK and just 12% in the US. US respondents are more likely to say they are using AI in specific use cases (34%) and also the most likely to say they don't intend to use AI in cybersecurity in the foreseeable future (9%).

The correlation between preference for single vendor platforms and AI use is strong when we look at geographical data splits. Thirty-six percent of Australian respondents say they prefer to use a single vendor platform with no third-party integrations, compared with only 11% of US and 15% of UK respondents. Together with the high incidence of AI use across all operations in Australia, it seems likely that vendors are introducing AI features in their platforms, rolling out AI by default in that region.

Most US respondents (42%) prefer to take a best-of-breed approach to technology selection, with solutions working together. Ease of integration is clearly an important factor in the solutions they use. UK respondents are most likely to favor a single vendor platform approach with integrations only where necessary (39%), although 31% use a best-of-breed approach.

ThreatQuotient Take:

Enthusiasm for AI adoption may also relate to the resourcing challenges Australian respondents seem to be facing. They are more likely than other regions to be assessing automation ROI on the basis of employee satisfaction and retention, and 36% are diverting unused headcount budget to automation, implying they may be struggling to recruit cybersecurity resources. Increased automation and AI deployment may help to fill this resource gap.



Cybersecurity automation drivers reflect regional market conditions and challenges remain

In the UK, the top driver for adopting more cybersecurity automation is regulation and compliance, which reflects the intense regulatory environment in the EU.

Australia is more likely than the other regions to be adopting automation to combat a skills shortage, which signals the challenges of recruiting skilled cybersecurity specialists in the country. Respondents from Australia are also more likely to be automating incident response than other regions (40% are implementing this use case compared to a global average of 32%), in a bid to relieve pressure on stretched teams. In the US the top driver is increasing productivity.

Despite the region's current enthusiasm for cybersecurity automation, respondents in Australia report more challenges around it, with 31% experiencing technology issues, compared to a global average of 24.5%. Lack of budget, lack of trust in outcomes, and a lack of management understanding/buy-in are all more common in Australia than in the US and UK. This may also relate to their preference for single-vendor platforms – if the vendor they are using does not offer automation expertise, Australian organizations may be struggling to achieve the desired results. We anticipate that this combination of factors will result in Australia experiencing frustration around cybersecurity automation in the coming years.

UK businesses are most likely to report issues around lack of budget and technology issues, while US respondents complain of a lack of time.

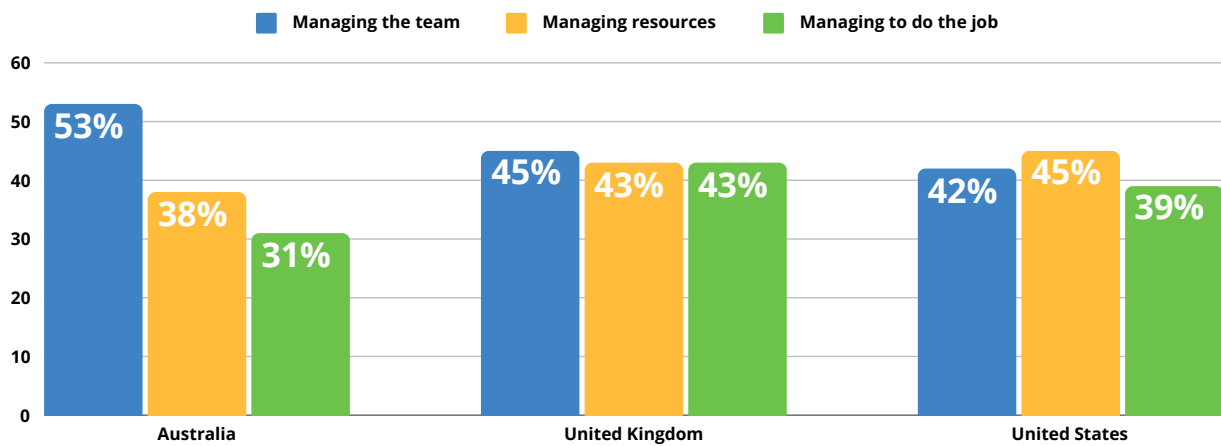
New budget is on the table

All regions report a similar level of increase in net new budget (39%). UK respondents are more likely to be diverting budget from other tools, while Australian respondents are allocating budget from outside security teams. Considering their documented skills gap, 36% of Australian respondents say they are allocating unused headcount to automation, but a similar percentage (37%) of UK organizations are also doing this. US respondents are less likely to be diverting budget from headcount (only 34% are doing this), or diverting it from other tools.

Performance and efficiency KPIs begin to erode employee well-being focus

The US is the only country that ranks how well they are managing resources in terms of efficiency/effectiveness and budget higher than employee wellbeing and retention (Figure 10). This has shifted considerably from last year, when employee satisfaction and retention were the preferred metric for 61% of US respondents; now just 42% say they use this to determine ROI. In the UK, employee satisfaction and retention remains the most popular ROI metric, but it is closely followed by how well the organization is managing resources and how well the team is doing the job in terms of mean time to detection and response. Australia is the only region where employee satisfaction and retention remains significantly ahead as a measure of automation ROI, underlining the recruitment challenges the region is facing.

Figure 10: Metrics used to measure cybersecurity automation ROI/KPIs (%)



VERTICAL SECTOR SNAPSHOT



Overall, the importance that organizations place on cybersecurity automation has risen, but there are variations between vertical sectors. Interestingly, its importance to financial services organizations has recovered strongly following a drop last year, and this year it is central government respondents reporting a drop.

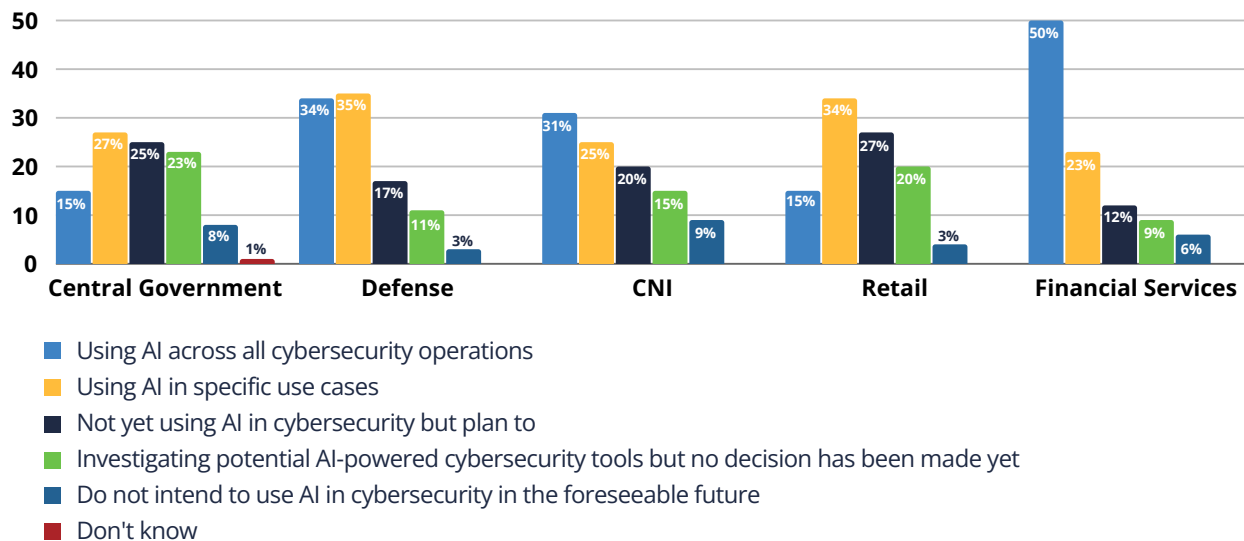
	2022	2023	2024
Central Government	71%	75%	71%
Defense	67%	73%	85%
CNI	71%	82%	81%
Retail	55%	77%	76%
Financial Services	75%	69%	87%

ThreatQuotient Take:

Financial services organizations tend to be more mature in cybersecurity automation adoption and may now have passed through the period of disillusionment that commonly occurs in the tech adoption cycle. Central government organizations are likely earlier into their adoption cycle and are now experiencing bumps in the road. Interestingly, central government respondents are more likely than those in any other sector to report problems with “bad decisions” – meaning their automation is not operating correctly – than any other sector.

Sector differences in the pace of new technology adoption are also evident when we asked respondents about the extent to which they are using AI in cybersecurity (Figure 11). Half of financial services respondents say they are using AI across all their cybersecurity operations and a further 23% are using it in specific use cases. In contrast, only 15% of central government respondents are using it across all operations and 27% in specific use cases. Defense organizations also show strong early adoption of AI, with 79% already using it to some extent. Retail is slower to adopt, with fewer than half using AI already.

Figure 11: Using AI in cybersecurity (%)





Automation use cases differ as deployments mature, but challenges remain

This year's study shows clearer differences between sectors in their preferred use cases for cybersecurity automation. Financial services respondents have a strong focus on incident response, phishing analysis, and threat hunting. Critical National Infrastructure respondents use it predominantly for threat hunting, threat intelligence management, and incident response. And, while phishing analysis is the top use case for central government respondents, they are also more likely than other sectors to leverage automation for alert triage (which was starting to feature in their top use cases last year) and vulnerability management.

Despite greater clarity on the use cases that work for their business, implementation challenges remain. Compared with 2023, where often two or three issues were identified as top challenges, there is greater consensus within vertical sectors about what the main challenge is. For defense and financial services respondents, technology issues are most prevalent, while critical national infrastructure respondents are experiencing a lack of budget. The dominant challenge for central government respondents is "bad decisions" e.g., where an automated process incorrectly blocks safe emails. Retail is the only sector that still has several almost equally difficult challenges, perhaps reflecting its lower automation maturity levels – in this case management understanding/buy-in is the main problem, but is closely followed by automation breaking systems, and lack of trust in outcomes.

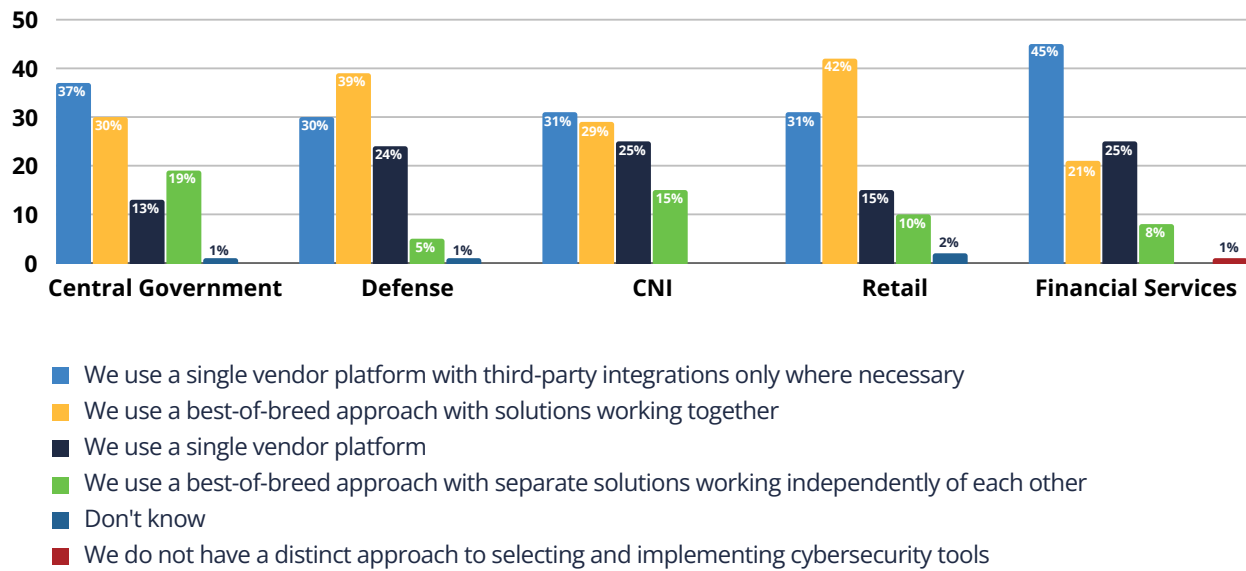
ThreatQuotient Take:

Organizations are homing in on what use cases work best for them. Previously, there has been a more even spread of automation deployment between use cases; this time respondents are clearer about where it is working for them. They are also clearer about where their challenges lie.

Sectors differ significantly on cybersecurity tools approach

Sector variations are strongly evident in how they select and implement cybersecurity tools (Figure 12). Seventy percent of financial sector organizations are firmly in favor of a single vendor approach, although 44% of these integrate third-party tools where necessary. In contrast, 39% of defense and 42% of retail respondents prefer a best-of-breed approach with solutions integrated and working together. The least popular approach is having best-of-breed tools working independently of each other, although 19% of central government respondents prefer this approach.

Figure 12: Approach to selecting cybersecurity tools (%)



ROI remains focused on team well-being

The majority of sectors use how well they are managing the team in terms of employee satisfaction/retention as the most popular ROI metric. Defense organizations strongly favor this approach - likely due to the challenges faced in gaining security clearance for new employees and the security risk related to high churn rates. The exception is central government, where respondents were more likely to use how well they are managing their resources and how well they're doing the job ahead of employee-related measures.

Threat intelligence sharing approaches vary

Threat intelligence sharing is a common activity across all industries, but there are variations in the audiences that intelligence is shared with.

Financial services, critical national infrastructure, and defense respondents are most likely to share intelligence with direct partners and suppliers, while central government and retail respondents are slightly more likely to share through an official industry threat-sharing community (Figure 13).

It is surprising that, despite the financial sector's well-established sharing communities and the upcoming intelligence-sharing requirements of regulations like DORA, financial sector respondents are the least likely to be sharing intelligence via their threat-sharing community.

Figure 13: Approach to cyber threat intelligence sharing (%)



Expected attack vectors reflect industry vulnerabilities

As we saw with regional variations in attacks of concern, the top attack types organizations expect to face vary by industry. This reflects the differences in motivations and vulnerabilities leveraged by threat actors to target specific sectors.

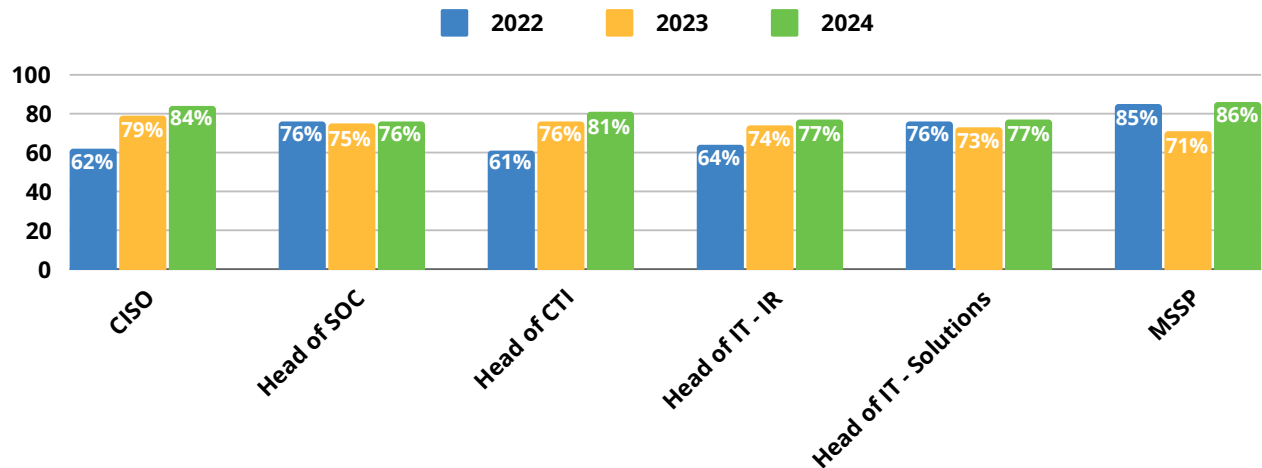
	Central Government	Defense	Critical National Infrastructure	Retail	Financial Services
1	State-sponsored attacks	Cyber-physical attacks	Cyber-physical attacks / attacks via our supply chain	IoT-based attacks	Ransomware
2	Phishing / Denial of service	Phishing attacks	AI-powered attacks	Phishing	Cyber-physical attacks
3	IoT attacks / attacks via our supply chain	AI-powered attacks	Ransomware / IoT-based attacks	Ransomware	Phishing

Role Variations

Our study once again surveyed a range of cybersecurity professionals including CISOs, Heads of SOC, Heads of Cyber Threat Intelligence, Heads of Incident Response, Heads of IT Security Solutions Architecture, and Managed Security Service Providers. While splitting the data by industry sector and region shows peaks and troughs in the importance associated with cybersecurity automation, among professionals the general trend is rising (albeit with a dip for MSSPs and security solutions architects in 2023) (Figure 14).

As previously, we see variations in the drivers for adopting cybersecurity automation. CISOs, MSSPs, and Heads of SOC are seeking productivity and efficiency almost equally, while Heads of CTI prioritize productivity. Heads of IT Security Solutions Architecture are the only group citing regulation and compliance as a top driver in this year's study.

Figure 14: Cybersecurity automation rated as important (%)



Cyber professionals are overcoming their trust issues and refining use cases as they bid for budget

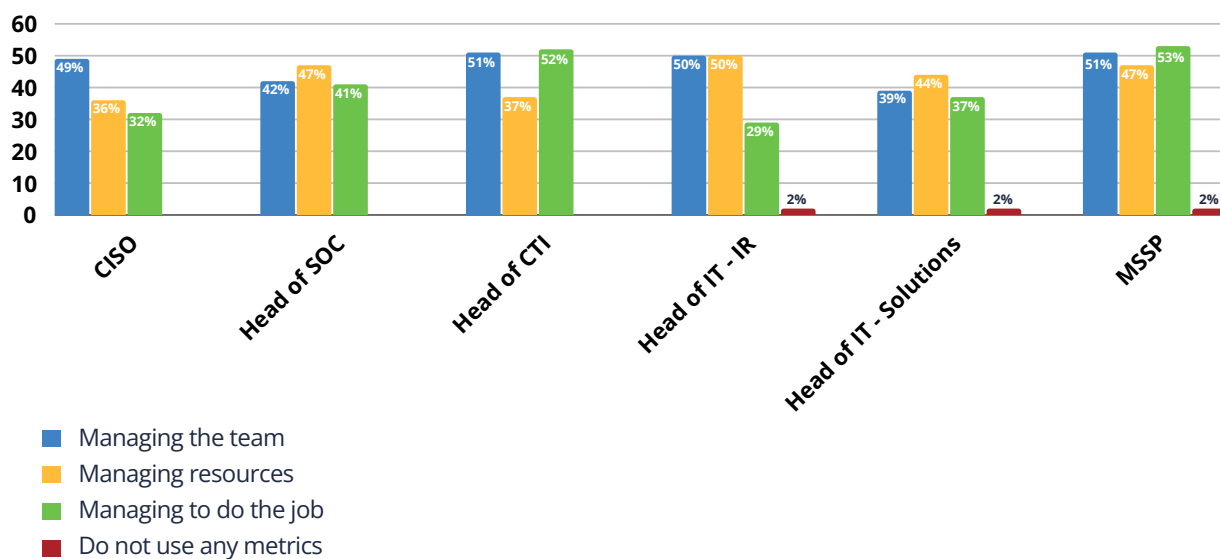
Last year, a lack of trust in outcomes was the top issue for Heads of Cyber Threat Intelligence, IT Incident Response, and IT Security Solutions Architecture. This year, only MSSPs report lack of trust as a notable problem, ranking it second after a lack of time. Instead, technology issues now feature as a common challenge across all roles. CISOs, however, say a lack of budget is the most common problem, and they're also the least likely to report getting net new cybersecurity automation budget, with just over one third (34.5%) doing so compared to an average of 39%.

In contrast, Heads of IT Incident Response (IR) are the most likely to be securing net new budget for automation. It's natural that Heads of IR are also the most likely to be using it to automate incident response (41% are doing so compared to an average of 32%), but they have clearly built a strong case and succeeded in gaining investment.

CISOs still prefer the human touch, but in other roles less human-centric KPIs are on the rise

There is a marked change across roles compared to last year, where cybersecurity professionals largely concurred on how to measure the ROI of cybersecurity automation and the majority were using employee satisfaction and retention. CISOs are now the only group leading with employee satisfaction and retention (Figure 15). Other roles are looking more closely at resource management – especially Heads of SOC and IT Security Solutions Architecture. There is far more focus on how well the job is being done from Heads of Cyber Threat Intelligence and MSSPs, too.

Figure 15: Metrics used to measure cybersecurity automation ROI/KPIs (%)



MSSPs lead the AI drive

Managed Security Service Providers are by far the most likely group to be using AI in cybersecurity. Ninety-four percent use some form of AI in cybersecurity and 65% use it across all operations. No other role comes close to this degree of adoption. Sixty-five percent of Heads of Cyber Threat Intelligence use it in some form. In all other roles only between 53% and 56% say they already use AI.

There are variations in how the different roles approach selecting and implementing cybersecurity tools. Heads of Cyber Threat Intelligence and Heads of Incident Response are most likely to favor a best-of-breed approach with solutions working together, while CISOs, MSSPs, and Heads of IT Security Solutions Architecture prefer a single vendor platform with third-party integrations when necessary. Heads of SOC are equally split between best-of-breed and single vendor platform approaches.

Threat Intelligence specialists are most keen to share

Those heading up cyber threat intelligence are the most likely to be sharing what they learn with others. At the sharp end of intelligence gathering and actioning, they clearly appreciate the power of collaboration. Sixty-two percent share information with direct partners and suppliers and 58% share through an official threat-sharing community. Nine percent go so far as to share intelligence outside their industry. Those in other roles are slightly less active in sharing intelligence. In fact, CISOs are more likely to share intelligence with others in their industry through a threat-sharing community (52% do this) than with their direct partners and suppliers (47%).

Heads of IR are the most likely to be sharing threat intelligence with others through unofficial channels – almost one-third do this, compared to one-quarter overall.

Expected attack types vary

When looking at attack types by role, concerns around cyber-physical attacks and phishing are prevalent across roles. However, as to be expected, those in roles of Head of IT Security and CTI that by nature are more forward, emerging attack types including deep fakes, AI-powered attacks, and IoT based attacks are of greatest concern.

	CISO	Head of SOC	Head of Cyber Threat Intelligence	Head of IT incident response	Head of IT Security solutions architecture	MSSP
1	Cyber-physical attacks	Phishing	Deep fakes	Cyber-physical attacks	AI-powered attacks	Ransomware
2	Phishing	Cyber-physical attacks	Cyber-physical attacks	Attacks via our supply chain	IoT based attacks	Phishing
3	DDoS attacks	Attacks via our supply chain	Malware	Malware	DDoS attacks/supply chain attacks/malware	Malware

ThreatQuotient Take:

Our study shows that different roles have differing views on automation. Where possible, professionals should collaborate to determine the most effective way to implement cybersecurity automation to achieve the organization's security and business goals.

ThreatQuotient Recommendations

As we consider the latest research findings on the evolution of cybersecurity automation in 2024, it's clear that cybersecurity professionals have grown more experienced, their skills have developed and they have adapted to the new normal of continuous, rapid change. Organizations have adopted cybersecurity automation as an important part of their defensive strategy, adopting more targeted, customized automation and use cases. However, even with this progress, significant challenges remain. Growing regulations and complex technology landscapes, the need to integrate with other third-party tools and the importance of refining strategies for sharing threat intelligence are all influencing cybersecurity professionals as they adapt to the new, constantly changing normal. 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 Don't believe the hype; Don't ignore potential utility:** As demonstrated through this report, the path to cybersecurity automation has gone through the typical hype cycle of enthusiasm and high expectations, followed by difficulties and disappointment, before landing on specific use cases that work for their organization. Focus on key use cases to ensure the "plateau" delivers the productivity needed.
- 2 Choose proven use cases for automation:** Focus on 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 - and securing the budget to support it.
- 3 Breadth and depth of Integrations are key:** Even if you prefer a single vendor platform approach you will need to integrate some third-party tools and feeds in order to get full visibility and control over the environment. Therefore organizations should seek out solutions that have integration capabilities designed in. This is an important aspect of a strong security practice and organizations should seek to build an ecosystem with breadth and depth, with the right solutions for particular use cases, with the necessary level of integrations. Clearly, flexibility and extensibility are critical, allowing tools to integrate easily into that ecosystem and result in a lighter management burden.
- 4 Broaden threat intelligence sharing for increased effectiveness:** While 99% are sharing threat intelligence in some form or another, when we look at the different channels for sharing, in each case the proportion using it is around 50%. With new regulations such as NIS2 and DORA putting emphasis on collaboration, organizations can show their support by looking at how to use automation to share valuable threat intelligence without adding to analysts' workloads. Sharing more broadly improves security posture for all.
- 5 Treat Automation and AI as scale functions:** Scaling cybersecurity is the next big challenge for organizations. Successfully uniting human expertise with AI and automation will help to improve employee morale, will increase productivity, reduce costs, and improve overall security posture.

ABOUT THE REPORT

This is the fourth edition of ThreatQuotient's annual survey of senior cybersecurity professionals, exploring the topic of cybersecurity automation adoption. Senior cybersecurity professionals in the UK, US, and Australia shared their views on the progress they are making toward adopting automation, its key use cases, and the challenges they face. It identifies trends and changes over time and charts how automation is maturing. This year's study also explores wider issues affecting the cybersecurity landscape such as AI adoption, commonly perceived threats, intelligence-sharing, and how organizations approach their cybersecurity tool strategy.

METHODOLOGY

Leading threat intelligence platform and security operations innovator, ThreatQuotient, commissioned a survey, undertaken by independent research organization, Opinion Matters, in June 2024. Respondents included 750 senior cybersecurity professionals in the UK, US, and Australia from companies employing 2,000+ people from five industry sectors: Central Government, Defense, Critical National Infrastructure – Energy and Utilities, Retail, and Financial Services.

About ThreatQuotient

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection, investigation and response (TDIR). ThreatQ is the first purpose-built, data-driven threat intelligence platform that 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 integration marketplace, data management, orchestration and automation capabilities support multiple use cases including threat intelligence management and sharing, incident response, threat hunting, spear phishing, alert triage and vulnerability management. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit www.threatquotient.com.