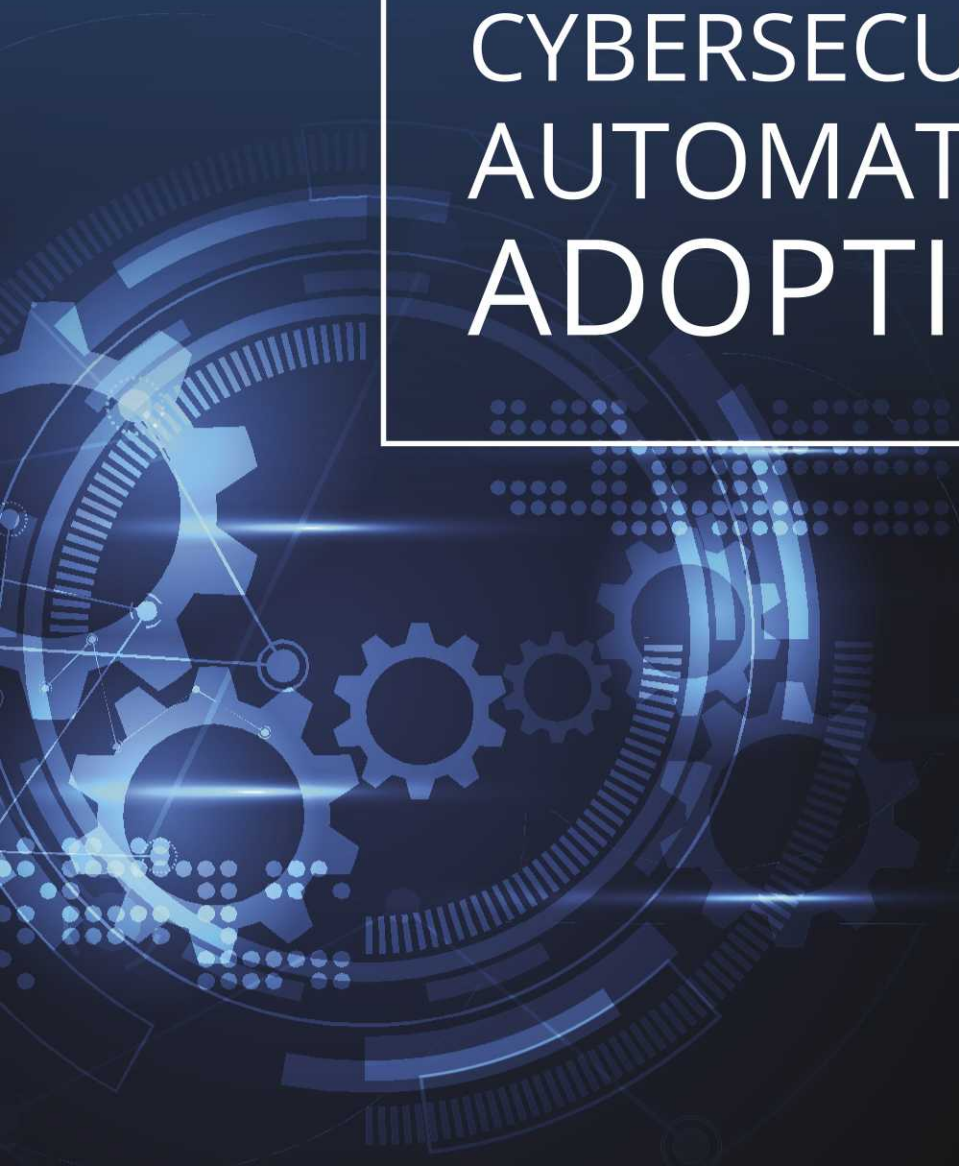
THREATQUOTIENT

STATE OF CYBERSECURITY AUTOMATION ADOPTION



www.threatquotient.com

CONTENTS

INTRODUCTION

This research was conducted to understand the importance, challenges and trends facing cyber businesses when it comes to automating their cybersecurity systems. It examines what cybersecurity use cases or processes organisations have already automated and what they are planning to automate, as well as any barriers organisations have overcome. It identifies the threat intelligence capabilities firms already have in place, and their future expectations. It explores budget, skills, resources and issues around trust and assesses the outlook for cybersecurity automation.

Read this report to discover how CISOs and senior cybersecurity professionals are planning to accelerate automating cybersecurity in different use cases as the global economy recovers from the pandemic. As the distributed workforce creates an expanded threat surface, organisations are looking at ways to automate their security systems to proactively mitigate escalating cyber threats while supporting a growing hybrid work environment. But do they trust in cybersecurity process automation and is a lack in trust holding them back?

METHODOLOGY

Leading security operations platform innovator, ThreatQuotient, commissioned a survey, undertaken by independent research organisation, Opinion Matters, in May 2021. 250 UK senior cybersecurity professionals from companies employing 2000+ people from a range of industries took part including:

CENTRAL GOVERNMENT

DEFENCE

CRITICAL NATIONAL INFRASTRUCTURE — ENERGY & UTILITIES

RETAIL

FINANCIAL SERVICES

FOREWORD

Gartner outlined how security and risk leaders must explore automation to provide increased business value and maintain security standards. Stating that automation is already impacting the world in two ways, first, as an enabler to the security and risk function and second, as new security frontiers that need to be acknowledged and understood, Gartner maintained that security professionals must deliver value using automation.

By combining automation with security intelligence, and applying that to existing infrastructure, an organisation can greatly improve its security posture.

The reality is that, as parts of the business continue to adopt emerging technologies ranging from cloud to AI and machine learning, digitisation and immersive technologies, security leaders will find themselves overwhelmed with data, differing requirements and the need to automate will be paramount.

But what do we mean when we talk about security automation? There are plenty of different definitions out there, but in our mind security automation is the machine-based execution of security actions with the power to programmatically detect, investigate and remediate cyberthreats — with or without human intervention. This is done by identifying incoming threats, triaging and prioritising alerts as they emerge, and responding to them in a timely way.

By using security automation security teams can eliminate a lot of the heavy lifting and more accurately address security alerts as they come in. By combining automation with security intelligence, and applying that to existing infrastructure, an organisation can greatly improve its security posture. In short, time-consuming activities are taken out of an organisation's security analyst team's workload so they can focus on higher value work such as threat hunting, strategic planning and conducting investigations, therefore bringing more value to the organisation. To this point, a study by Rapid7 showed that security teams can save up to 83% on time per alert by using security automation. Additionally, IBM reported that businesses with fully deployed security automation show a cost-saving difference of £2.6 million in a data breach scenario compared to companies that have yet to deploy advanced technologies. This cost gap has grown by £1.5 million since 2018. And, according to the Global Security Automation Survey, 38% of surveyed organisations reported a medium level of automation in 2020, higher than the 2019 level of 34%, showing that organisations are becoming more willing to automate their security processes.

So, why aren't more organisations automating the majority of their cybersecurity systems?

To gain a clearer picture of the state of cybersecurity automation and adoption, and understand what is either accelerating or holding UK PLC back, we commissioned this survey to understand how far down the road senior cybersecurity professionals are with their cybersecurity automation initiatives.

Our research showed that 95% of respondents have automated at least some of their processes with 67% automating between 25 and 100% of their processes and that 98% intend to automate more in the next 12 months, which is good news — right?

Not exactly. There are several barriers that are preventing organisations from maximising the benefit of automation, such as budget, prioritisation issues, talent gaps, technology, trust concerns and fears around lack of control and the risk of automating the wrong tasks, and more. It is clear from the research that process driven automation creates issues around lack of trust, and that respondents often feel this can lead to bad decisions.

> Here at ThreatQuotient, we know that data driven automation can enable security operations teams to reliably trust the data and be confident in their decisions, which for many security professionals will be absolutely groundbreaking as they look to automate more use cases.

We hope you enjoy reading the report.

HIGH LEVEL FINDINGS

77%

say automation is important

95%

use automation 98% plan to use more automation

92%

experienced problems

41%

lack trust in the outcomes

The importance of cybersecurity automation

Cybersecurity automation is important to senior security professionals, with three quarters of the survey respondents (77%) stating this to be the case.

Overall intentions to automate were high, with **95% stating that they have automated to some extent,** and a trailblazing 40% saying they have automated between 51 and 100% of their processes. Additionally, **98% are planning to automate more of their security estate in the next 12 months.** Of these, 5% will be applying automation for the first time.

Is the desire to automate being inhibited by doubt and fear?

According to a third (34%) of survey respondents, the top reason for cybersecurity automation is the need to improve or maintain security standards. Interestingly, this was closely followed by a lack of trust in cybersecurity automation (31%) and the need to improve efficiency and productivity (31%). This begs the question as to why this lack of trust is so high and why the desire to automate is being inhibited by doubt and fear? **Doubt about the accuracy of the detection of threats, and fear of the consequences of automating the containment or mitigation responses and the prospect of detrimental impact and damage resulting from doing this incorrectly.**

What's required for cybersecurity automation to be successful?

Going forward for cybersecurity automation to be successful, more than half (51%) of the survey respondents said that **well-defined manual processes were required.** This was closely followed by integration between vendor technologies (47%).

Half of the survey respondents are automating threat intelligence

The good news is that half of the survey respondents are already automating threat intelligence processing and 44% are automating vulnerability management, with 39% automating password resets. Intention to automate threat intelligence was also cited as the top use case for applying automation in the future.

Top blockers

Interestingly, technology was cited as the top blocker that is preventing organisations from applying cybersecurity automation, with 43% of respondents stating this. This was followed by budget (40%) and then skills (36%). Therefore, it would seem from these responses that organisations that have automation capabilities built into technologies such as SIEMs, Endpoint Detection & Response and Security Automation & Orchestration solutions appear not to trust these to automate much beyond basic tasks such as sending out notifications or running a threat intelligence query.

Challenges to cybersecurity automation

To this point, 92% of organisations have experienced problems/issues when implementing cybersecurity automation. In fact, only 8% said that they had not experienced problems. **The biggest problems have arisen from a lack of skills (45%) and a lack of trust in the outcomes (41%).** Budget was cited as the third biggest problem encountered. Is there a requirement here for senior security professionals to develop clearer RoI around automation to enhance and support the business case for budget?

VERTICAL MARKET SNAPSHOT

The research also examined responses from five key vertical markets including: Central Government, Defence, Critical National Infrastructure — Energy and Utilities, Retail and Financial Services. Here is a snapshot of some of the key findings:

Central Government

- When selecting an cybersecurity product, 38% of Central Government said that atomic actions that take place inside one system, such as automatically creating a ticket, were critically important and 40% said they were fairly important. Likewise, 40% of respondents from this sector also rated complete automated workflow orchestration as critically important.
- For cybersecurity automation to be successful, 64% of Central Government respondents rated having well defined manual processes as the most important factor. This was higher than other sectors surveyed, where the average was 51%.
- Increasing productivity was a top driver for adopting cybersecurity automation for 56% of Central Government respondents. The most common cybersecurity use case that is already automated in Central Government is vulnerability management, selected by half of respondents. Half are looking to automate incident response and management in the future.
- In terms of what is preventing organisations from applying cybersecurity automation, half of Central Government respondents said budget and skills.
- When asked about the problems that they have encountered 46% said they had made bad decisions as a result of cybersecurity automation, which was much higher than the industry average of 30%.

Defence

- When asked about the main driver behind the adoption of cybersecurity automation, 60% of Defence respondents said that this was about increasing productivity, which was higher than the other surveyed sectors.
- In the next 12 months, 58% of respondents in this sector said that they are planning to automate third party integrations and associated processes. Additionally, 54% said they are planning to automate data cleansing and extraction.
- 34% of Defence sector respondents admitted that they are struggling to get management understanding and buy in, a percentage which was higher than the other sectors.
- Currently 34% of Defence sector respondents have automated up to 25% of their processes and intend to automate more in the next 12 months.
- In terms of the problems experienced, half of Defence sector respondents admitted to a lack of trust in outcomes.

Critical National Infrastructure — Energy & Utilities

- Only 14% of Critical and National Infrastructure respondents rated cybersecurity automation as very important which was the lowest out of all vertical sectors surveyed.
- When asked what is required for cybersecurity automation to be successful, half of respondents said well defined manual processes.
- When respondents were asked which part of their threat intelligence capability they are planning to automate, over half (54%) said data prioritisation and 52% are planning to automate enrichment.
- A key driver for cybersecurity automation for over a third (38%) of respondents in this sector was 'improving and maintaining cybersecurity standards.'
- When asked about the problems they have encountered, 48% of respondents admitted to a lack of trust in outcomes.

Retail

- Out of the vertical markets surveyed, respondents from the retail sector were most likely to state that IT automation was very important, with 36% saying this.
- However, 46% of retail sector respondents have encountered a lack of skills and 38% a lack of budget when trying to implement cybersecurity automation which was higher than the other sectors surveyed.
- For cybersecurity automation to be successful over half (58%) of retail respondents said integration between vendor technologies was required. To this point 48% said that they had already automated third party integrations and associated processes.
- A key driver for nearly half of respondents in this sector (46%) is the 'drive to improve and maintain cybersecurity standards'.
- In terms of specific use cases that retail respondents have already automated, 60% said threat intelligence processing and 48% said vulnerability management.

Financial Services

- The Financial Services sector was the second highest of the five verticals to say that IT automation was very important, with 30% stating this.
- As you would expect, regulation and compliance was a key driver for over one third (36%) of financial services respondents. Outside of this the top driver for Financial Services respondents was increasing productivity (46%).
- In terms of use cases nearly half (48%) already automate third party integrations and associated processes and more than half have already automated data prioritisation (52%) and over half (58%) said that they want to apply automation to vulnerability management.
- Overall, in terms of problems encountered, lack of skills was a key issue for half of the Financial Services respondents, this was followed by lack of trust in outcomes (36%).

RECOMMENDATIONS

Unfortunately, dependencies, complexities, a lack of trust and many unknowns are the bane of cybersecurity automation. Having said that, any incident or vulnerability must be addressed swiftly and accurately, especially as the threat surface continues to expand, and automating use cases will be key to this. Based on the research findings, here are six key recommendations that senior security professionals should follow if they are looking to automate their security processes:

1. It is important to understand what you want to achieve and how you are going to achieve it. Just buying technology is not going to solve your problems.

2. Skills and resources were highlighted as an issue by respondents, therefore look for cybersecurity automation technology where professional security services are also provided. This will help you understand your security processes better and also provide you with programming expertise if and when required.

3. Automation needs to be data driven rather than process driven — work with a provider that can help you focus on the threats that matter to make better decisions faster and respond more efficiently and effectively.

4. Organizations should not automate everything, otherwise it can become too noisy. They should contextualize first to understand and ensure the relevance before automating actions. This will give teams more confidence in the data, decisions and actions.

5. Remember you can expand automation as trust and confidence increases, across different use cases.

6. Look for a data driven security operations platform that is purpose built for threat detection and response.

MAIN SURVEY QUESTIONS

1. How important is cybersecurity automation to your organisation?

Overall, three quarters (77%) of respondents stated that cybersecurity automation is important to their organisation. 26% said it is very important, 51% said somewhat important. Only 6% said either somewhat unimportant or not important at all.

When looking at the different roles surveyed, Heads of cybersecurity Solutions Architecture scored highest with 94% rating security automation as important to some degree, among whom 33% said it was very important and 61% said somewhat important. This was followed by Head of IT Incident and Response with 37.5% saying this was very important and 50% saying somewhat important. Whereas only 28% of CISOs said that cybersecurity automation was very important and 43% said it was somewhat important. Surprisingly, 70% of the Heads of Security Operations respondents viewed automation as only somewhat important, with only 4% saying it was very important.

Respondents from the Retail sector were most likely to state that IT automation was very important, at 36%. This was followed by Financial Services with 30%, whereas only 14% of Critical and National Infrastructure respondents rated it as very important.

2. How important in relation to these scenarios is automation to your organisation when selecting an cybersecurity product?

When selecting an cybersecurity product, 63% of respondents said that atomic actions were either fairly or critically important — 23% said they were critically important and 40% of respondents said they were fairly important. 66% said that partial automated workflow orchestration was critically or fairly important, with 18% claiming it to be critically important, and 60% stated that complete automated workflow orchestration was critically (22%) or fairly (38%) important.

38% of Central Government respondents rated atomic actions as critically important and 40% said it was fairly important.

30% of Heads of IT and Incident Response respondents rated this highly. This role is often reactive, time critical and high profile and is why atomic actions are rated so highly by these respondents.

20% of Financial Services respondents rated partial automated workflow automation as critically important and 27.5% of Heads of IT and Incident Response respondents rated this highest.

40% of Central Government respondents rated complete automated workflow orchestration as critically important. 28% of Heads of cybersecurity Solutions and Architecture rated this highest.

Note — Definitions

Atomic actions that take place inside one system, such as automatically creating a ticket.

Partial automated workflow orchestration, that updates multiple systems and products but involves human intervention to either initiate or approve the action(s) taken.

Complete automated workflow orchestration, with design logic, that updates multiple systems and products without any human intervention.

3. In your opinion, what is required for cybersecurity automation to be successful in your organisation? (Tick all that apply)

Over half of respondents (51%) said well-defined manual processes were required for cybersecurity automation to be successful. This was closely followed by integration between vendor technologies (47%). Regarding other factors, 43% stated additional in-house DevSecOps resources and 38% said in-house programming knowledge were needed for cybersecurity automation to be successful.

Government sector respondents (64%) were more likely than other sectors to say well-defined processes were a requirement for IT automation success, while integration between vendors was highest for Retail respondents (58%). Well-defined manual processes was the requirement for success most selected by CISOs, whereas Heads of the Security Operations Centre rated in-house programming knowledge highest (52%). 65% of those in Incident Response roles rated integration between vendor technologies.

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

The top driver behind respondents' need to adopt more cybersecurity automation was increasing productivity (53%) this was followed by improving or maintaining cybersecurity standards (34%) which was then closely followed by lack of trust in cybersecurity automation (31%) and the need to increase efficiency (31%).

This begs the question as to why the lack of trust in cybersecurity automation is driving organisations to adopt more technology — which seems counterintuitive; if you don't trust technology, why add more? However, we believe that security professionals feel they need more intelligence to foster greater trust in the data and that process driven automation is not working and this is where we advocate that data driven automation is a much better approach.

Other key drivers cited include skills shortages and regulation and compliance which were both chosen as top drivers by 30% of respondents.

Increasing productivity was a top driver for Defence respondents (60%) followed by Central Government.

Regulation and compliance was high for Central Government (38%) followed by Financial Services (36%).

Retail respondents scored highest in the category (46%) 'improving and maintaining cybersecurity standards'. Critical National Infrastructure also scored high in this category with 38%.

For CISOs increasing productivity, efficiency and maintaining cybersecurity standards all tied at the top with 31% respectively. Whereas for the Head of IT Security Solutions Architecture skill shortages was the top driver for 43%.

5. What, if any, cybersecurity processes / use cases do you automate today in your organisation? (tick all that apply)

Half (50%) of the respondents we surveyed are already automating threat intelligence processing. 44% are automating vulnerability management and over one third (39%) password reset, with 38% ticking incident response. Here it is important to note that threat intelligence processing benefits greatly from a data driven approach.

Threat intelligence processing was most likely to be already automated in Retail (60%) followed by vulnerability management (48%). Vulnerability management was highest in Central Government (50%), followed by password reset (48%).

56% of Heads of IT Security Solutions / Architecture said they automate threat intelligence processing which was higher than other roles.

6. What, if any, cybersecurity use cases / processes does your organisation want to apply automation to in the future? (tick all that apply)

In terms of cybersecurity use cases or processes that organisations are looking to automate in the future, threat intelligence processing came out highest at 49% followed by incident response and incident management (46%) and vulnerability management 39%.

Interestingly password reset was lowest at 33%, perhaps indicative of the fact that 39% of organisations have already implemented this.

Threat intelligence processing was highest in Retail and Defence, and both sectors had 54%.

Financial Services scored higher than any other sector and the overall average in vulnerability management with 58%.

Central Government and Retail scored highest on incident response and incident management with 50% respectively.

7. Which parts, if any, of IT's threat intelligence capability is your organisation looking to automate in the next 12 months, or has already automated?

	Already automate	Plan to automate	Neither
Third party integrations and associated processes	**40%**	**47%**	**14%**
Retail and finance scored highest on already automated	48%		
Defence scored highest on planning to automate		58%	
Utilities scored highest on saying neither			30%
Data management	**44%**	**42%**	**13%**
Retail scored highest on we have already automated	52%		
Government scored highest on planning to automate		48%	
Utilities and Defence score joint highest on saying neither			18%
Data prioritisation	**42%**	**45%**	**13%**
Finance scored highest on we have already automated	52%		
Utilities scored highest on planning to automate		54%	
Utilities scored highest on saying neither			16%
Enrichment	**36%**	**48%**	**16%**
Finance scored highest on already automated	46%		
Defence and Utilities scored highest on planning to automate		52%	
Central Government scored highest on neither			20%
Data cleansing and extraction	**40%**	**46%**	**14%**
Finance scored highest on already automated	60%		
Defence scored highest on planning to automate		54%	
Central Government scored highest on neither			26%

8. What, if anything, is preventing your organisation from applying cybersecurity automation? (tick all that apply)

Interestingly, technology was cited as the top blocker preventing organisations from applying cybersecurity automation, with 43% of respondents stating this. This was followed by budget (40%) and then skills (36%). Other notable blockers were resources (32%), management understanding and buy-in (31%) and time (25%).

Retail scored highest on technology (48%) followed by the Defence sector with 46%. Central Government scored budget and skills highest (at 50% respectively). Defence scored highest on management understanding and buy-in, at 34%.

It was interesting that budget was such a common problem; this may mean that senior security professionals need to be able to better demonstrate the RoI that can be achieved through automation in order to compete for budget. Cybersecurity automation could be losing out to other technologies and viewed more as a nice-to-have rather than a must-have.

For Incident Response professionals, 57.5% rated technology as a top blocker.

9. Has your organisation already automated parts of its cybersecurity processes and what is it intending to do over the next 12 months in relation to cybersecurity automation / projects?

It is clear from the majority of the respondents surveyed that automation is ongoing, it is a continuous process which needs investment.

95% have already automated somewhere between up to 25 and 100% of their processes and 98% are planning to automate more in the next 12 months.

Over a quarter (28%) have automated up to 25% of their processes and intend to automate more and 27% stated that they have automated between 26 and 50% and intend to automate more. 16% have automated 100% of their processes and intend to automate as their needs change over the coming year.

34% of Defence respondents have automated up to 25% of their processes and intend to automate more.

32% of Retail and 28% of Central Government respondents said they have automated between 51 and 99% of their processes and intend to automate more.

36% of Critical National Infrastructure respondents have automated between 26 and 50% of their processes and intend to automate more.

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

9 out of 10 or 92% of organisations have experienced problems and issues when implementing cybersecurity automation and only 8% said that they had not experienced problems.

The biggest problems have arisen from a lack of skills (45%) and a lack of trust in the outcomes (41%). Budget was cited as the third biggest problem encountered. Other notable problems encountered included that 30% felt that it had resulted in bad decisions and 22% said that it had led to them breaking systems. The lack of trust in the data is clearly an issue that senior security professionals are grappling with.

Interestingly CISOs rated lack of trust in outcomes as the biggest problem that they experience with 41% saying this.

Lack of skills was the biggest problem encountered in Central Government and Financial Services with 50% of respondents from both sectors saying this. Making bad decisions was most often encountered in Central Government, at 46%, which was a lot higher than the average of 30%. Defence scored highest in saying they had a lack of trust in outcomes (50%) whereas respondents from the Retail sector scored highest in citing lack of budget.

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 and APAC. For more information, visit **www.threatquotient.com**.