

Threat Detection 2024:

# Rejuvenating Cyber Defence Strategies.



# Table of contents

<b>Foreword</b>	3
<b>Research methodology</b>	3
<b>Introduction</b>	4
<b>Are outsourcing providers alleviating CISO burnout?</b>	5
Alignment to CISO priorities	6
The rise of hybrid teams	7
Security teams want more proactivity	8
Three questions you should ask your supplier to drive more value	8
<b>The benefits of SOC-as-a-service are not being fully realised</b>	10
Commercial frustrations around SOC-as-a-service	12
Lack of threat-hunting capabilities	13
How to demonstrate security effectiveness to the board	13
The desire to outsource is still there	14
<b>Mid-size organisations fare the worst</b>	15
Flexibility and transparency is lacking	16
Specialist expertise	17
Confidence	17
Five fundamentals regardless of company size	18
<b>Cyber defence rejuvenation in 2024</b>	19
Providers will need to prove their value	20
Security teams will relinquish more control to trusted providers	20
Contracts will be more commercially flexible	20
Service and tooling flexibility becomes more of a priority	21
Quality cyber defence will become more accessible	21

Ransomware is the largest cyber threat for all companies in 2023. The escalation of commercially and politically fuelled cyber-attacks means that businesses globally are battling with ransomware attacks – and their catastrophic impacts – on a daily basis. We are in the privileged position where e2e-assure, for the past 10 years, has been assisting companies to avoid these scenarios and we repeatedly get called upon to help in the aftermath of such an attack. This has raised the questions; are current cyber defences good enough and are cyber security providers currently failing UK businesses?



We commissioned this research involving 500 CISOs and senior security decision-makers from a variety of industries to find out. It reveals some alarming findings around the current offering from cyber security providers and highlights what CISOs and cyber security decision-makers want from their providers in 2024 to ensure they are best protected against the advancing threat.

**Rob Demain**  
CEO e2e-assure

## Research methodology

The research was conducted by Censuswide, on behalf of e2e-assure, surveying 506 CISOs and cyber security decision-makers with between 500-5,000 employees. Censuswide abides by and employ members of the Market Research Society which is based on the ESOMAR principles.

# Introduction

Only 22% of the CISOs and cyber security decision-makers who took part in this study describe their organisation as resilient.



A significant  
**42%**

said that their cyber security operation – whether managed by a provider or in-house is underperforming.

2023 is proving to be another monumental year for cybercrime. With continuous year-on-year growth in reports of data breaches and cyber-attacks, it is evident that the cyber threat to businesses is unrelenting. Our survey reveals that the vast majority (75%) of CISOs and cyber security decision-makers have experienced a cyber-attack, with most organisations stating they either fully outsource (45%) or have a hybrid approach (34%) to managing their security operations.

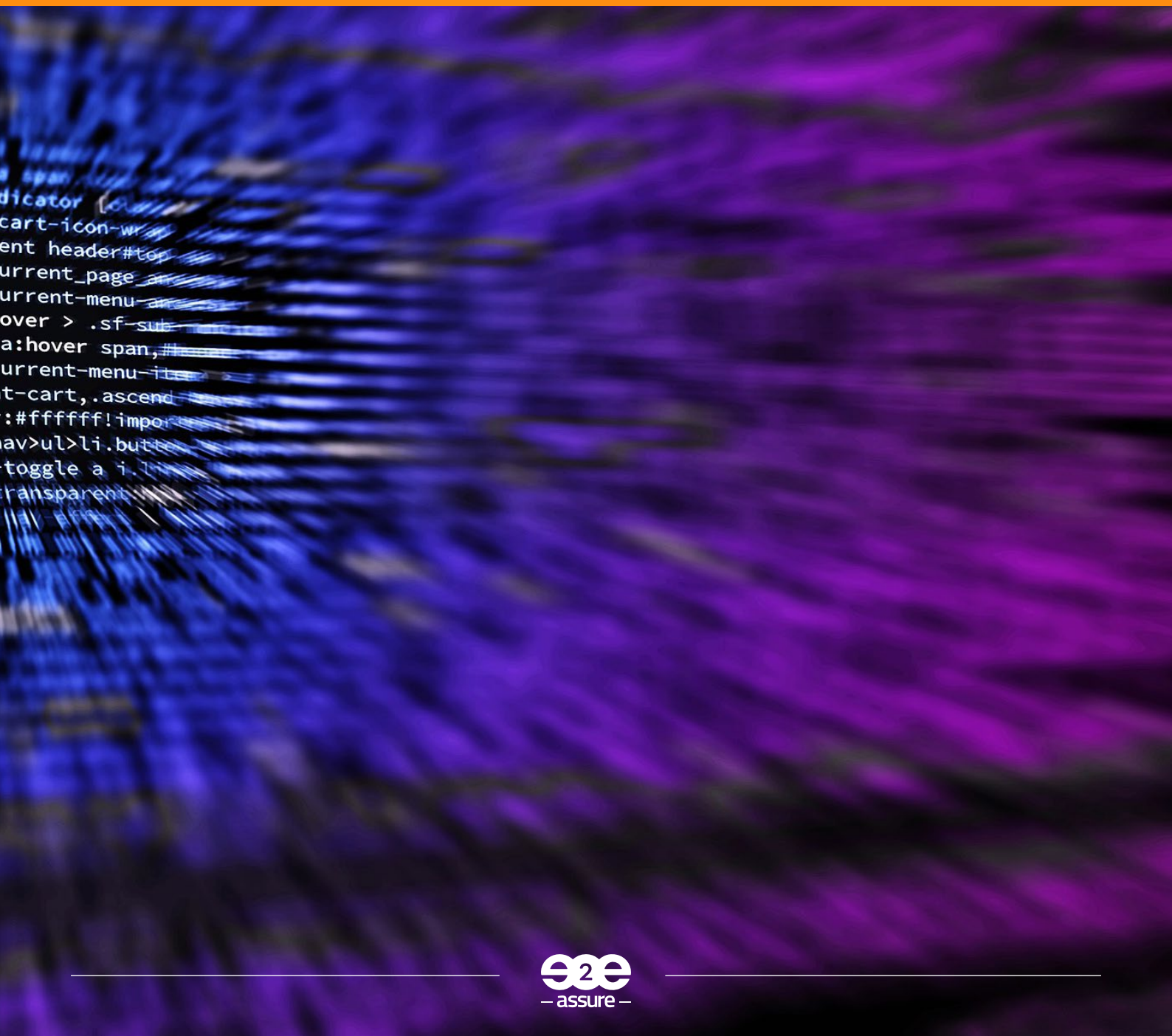
Our survey reveals that the majority (73%) of respondents are confident overall in their organisations' ability to act and respond to security incidents within 30 minutes, with 59% of respondents feeling that their security posture is much improved. Only 16%, however, said their provider or in-house team has exceeded their expectations, with 42% of respondents feeling 'ok'

about their provision, acknowledging that there is 'room for improvement'.

Within this research, we delve into observations from CISOs and decision-makers calling for a shift in tackling today's cyber challenges. We explore the top areas for improvement and how organisations can challenge their provider to create a more resilient future.

Chapter 1

# Are outsourcing providers alleviating CISO burnout?



Organisations that fully outsource their security operations (45%) predominately choose to so that they can gain access to specialist expertise as well as advanced tools and techniques to detect and respond to threats.

# 59%

reporting that their provider is underperforming and will be looking to make changes



However, our research suggests that those currently outsourcing, are not reaping the expected benefits with over half (59%) reporting that their provider is underperforming and will be looking to make changes.

Organisations currently outsourcing are also less confident in their ability to respond to a threat within 30 minutes (40% vs 45% of those that manage it in-house) and less likely to classify their provision as 'resilient' compared to in-house teams (21% vs 34%).




**40% vs 45%**

of those that manage it in-house and less likely to classify their provision as 'resilient' compared to in-house teams

**21% vs 34%**

## Alignment to CISO priorities

When asked about their priorities, CISOs are looking for

-  greater speed (45%),
-  more control (35%),
-  better resilience (29%),

from their security provision, yet we

found it was the in-house teams who were more aligned to these attributes. In-house teams currently provide stronger accountability with agreed SLAs and KPIs (54% vs 46% who fully outsource), and more commonly provide real-time visibility of reporting dashboards (53% vs 43%). This suggests that outsourcing providers are lagging in sufficient governance to provide CISOs with the clarity, precision and control they are looking for.

Whilst providers have made large strides from a commercial and contractual perspective, a large proportion of CISO's still desire



flexible (50%) & rolling (43%) contracts,



transparent pricing (44%),



stronger client centricity (43%),

from their delivery, evidenced through more effective communication and account management.

As a result, only 23% of those that currently fully outsource say they will continue to do so, with 28% planning to bring their provision back in-house and 25% looking for specific expertise as opposed to a full outsource. This puts into question the current effectiveness of outsourcing relationships and whether providers are alleviating or adding to CISO burnout.

## The rise of hybrid teams

# 61%

What is evident from our study, is the rise of hybrid teams, bringing together the best from both in-house delivery and outsourcing. Those who currently adopt a hybrid model are the most likely to continue with their existing operating model, with 61% expected to continue leveraging a hybrid approach and specialist expertise.

Hybrid organisations are the most confident with their use of threat detection, can attest to more regular testing (48%), and have the most intuitive and tailored detection rules in place (66%). The majority (80%) are also confident that

expected to continue leveraging a hybrid approach and specialist expertise

they could act and respond to an alert within 30 minutes.

As we revisit the CISO's priorities of speed and control, it would appear hybrid and in-house delivery models are most effectively supporting this. Comparably, if we review the overall impact of outsourcing fully, our study fails to support the notion of it having significant enough benefits to alleviate CISO burnout.

# Security teams want more proactivity

Despite the number of disappointed CISOs across our sample, it is clear there is an appetite from CISOs to pass more responsibility to providers. CISOs are largely happy to pass over more responsibility to



gain quicker decision-making (70%),



gain faster response times (68%),



achieve cost efficiencies (67%),



reduce the reliance on their team (63%).

This suggests that factors such as proactivity and ownership play a key role in CISO disappointment and highlights a missed opportunity for providers who could be doing more to support their clients.

## Three questions you should ask your supplier to drive more value

At any given time, a CISO must have an accurate and up-to-date view of the security posture of the organisation.

Efficient cyber security reporting is integral to understanding this. The ability to see the detail required as quickly as possible will increase both the efficacy of this reporting and the organisation's resilience by aiding faster decision-making.





Here are three questions you should be asking:



## How will you demonstrate that you've made our organisation a harder target for cyber criminals?

By tracking emerging threats and vulnerabilities and using a combination of proactive measures, your provider should be able to effectively analyse your security stance against the evolving threat.



## Can you measure how long it will take for an attacker to successfully compromise our organisation?

Here your provider should be able to deliver KPIs including the mean time to detect, mean time to contain and mean time to provide analytics. These should be quantifiable, providing an average time to classify and neutralise an incident including relevant threat intelligence.



## How will you evaluate our organisation's security stance on an ongoing basis?

Your provider should evidence a continuous approach to security validation, through methods such as attack simulation to mitigate security gaps quickly.

Asking the right questions of your provider is key to driving more value.

## Chapter 2

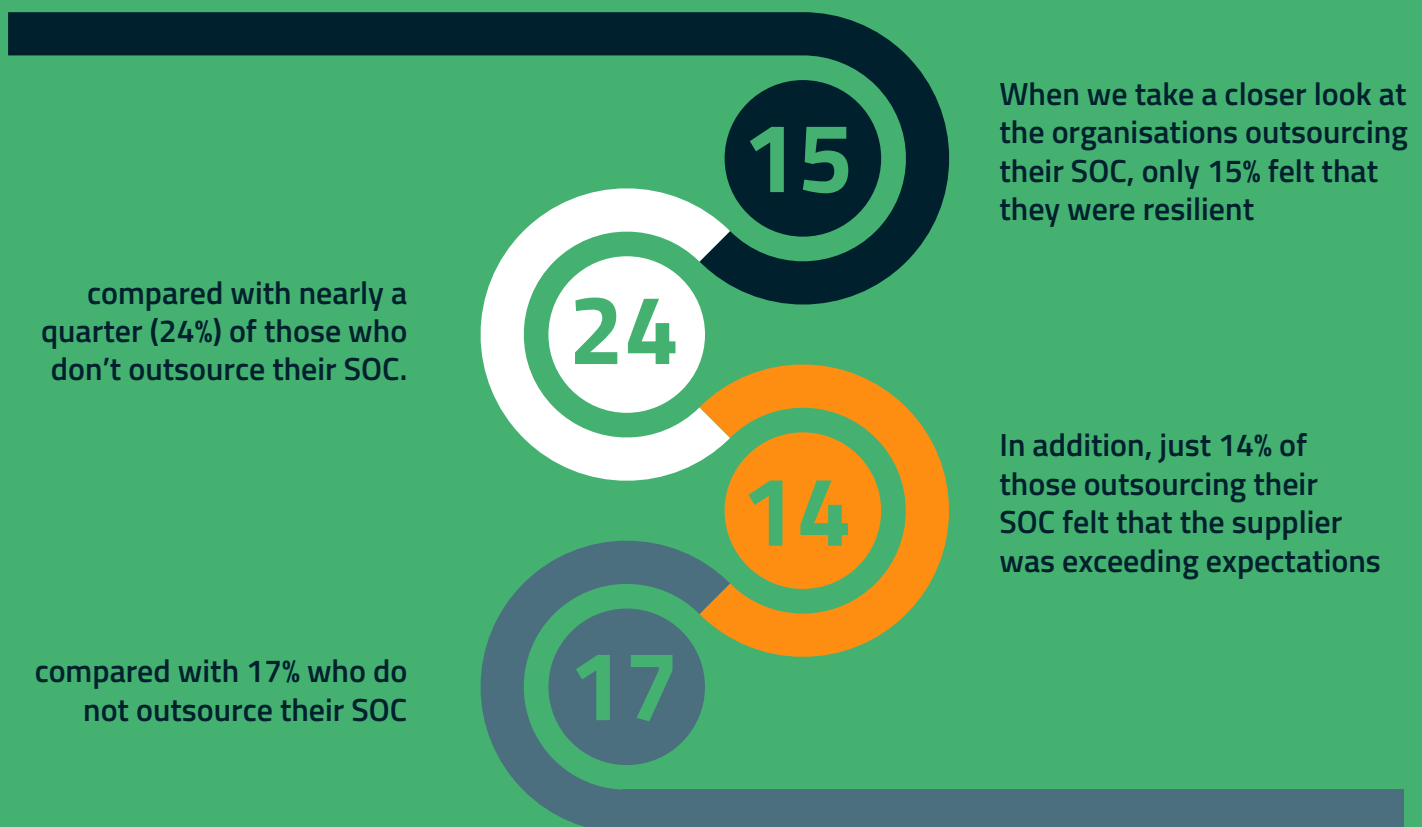
# The benefits of SOC-as-a-service are not being fully realised

---



Globally, the SOC-as-a-service market is predicted to grow from \$6.7 billion in 2023 to \$11.4 billion by 2028. With a CAGR of 11.2%, it is a high-growth area of the cyber landscape, and a competitive one too. Our research reveals it remains one of the top three most popular cyber security operations to outsource (29%) and that adoption has largely been driven by the enterprise (51%), followed by mid-size companies (28%).

However, more than one in three (36%) who outsource their SOC as part of a SOC-as-a-service model say that it is underperforming.



When we take a closer look, only 15% felt that they were resilient, compared to nearly a quarter (24%) of those that do not outsource their SOC. In addition, just 14% of those leveraging SOC-as-a-service felt that the supplier was exceeding expectations, compared to 17% of those that do not outsource their SOC. This highlights that

even when outsourcing specialist areas such as SOC-as-a-service, the benefits are not being fully realised.

Our study points to two areas where SOC-as-a-service providers could be more effective in exceeding CISO expectations.

# Commercial frustrations around SOC-as-a-service

Long and predictable contracts have been the standard within the cyber security landscape for decades. While for some they allow for predictable costs, they also restrict the degree of flexibility and agility over a contract term. It is therefore not surprising that this was cited as the main frustration by respondents that leverage SOC-as-a-service (37%). It is also clear from the research, that this frustration has follow-on consequences too, with organisations struggling to ensure that their cyber provision continues to be fit for purpose.

Such rigid contracts appear to cause issues when requirements expand beyond the original statement of work, resulting in a continual need to bolt on new security options (32%) rather than just an evolution

of the original contract. This is not ideal for security teams given the process of onboarding new services can be expensive and clunky, therefore restricting their agility.

## Main frustrations:



long contracts



bolt ons



threat hunting capabilities

# Lack of threat-hunting capabilities

Threat-hunting capabilities, or lack thereof, is the second frustration cited by organisations who use SOC-as-a-service. There was a marginal difference (1%) in the level of frustrations felt around implementing proactive measures such as threat-hunting to best tune alerts and protect the environment, between those that outsource their SOC (27%) and those that don't (26%).

These capabilities are even lacking in security operations that are deemed to be 'exceeding expectations', with 45% of these respondents unconfident in their provider's current use of threat intelligence. This highlights that few benefits are being realised by bringing in dedicated, specialist expertise and outsourcing this service.



## How to demonstrate security effectiveness to the board

Regularly testing security operations allows CISOs to verify that the organisation is capable of effectively monitoring and responding to security threats. It also allows the CISO to demonstrate to the board that investment in the SOC is worthwhile and can provide intended security benefits.

To make sure that your provider can shield your organisation from the advances of cyber criminals, challenge them to challenge your cyber strategy.

# Here are five key checks your provider should be regularly carrying out:

1. Continually validate the data source to check things such as log configuration and log availability.
2. Continually validate the analytics to ensure that threat data is accurate.
3. Enhance cyber capabilities through consistent feedback and knowledge transfer.
4. Test processes for the organisation to fall back on in the event of a breach.
5. Show trends over time to show improvements.

In addition to identifying any weak spots and potential attack paths, continuous testing also provides transparency of the organisation's security posture, which should be wrapped into a single dashboard that's easy for the board to consume and navigate.

## The desire to outsource is still there

On the positive side, respondents cite that SOC-as-a-service suppliers excelled in innovation (**70% vs 57% who did not outsource their SOC**). This may signal that respondents anticipate their provider delivering benefits further downstream.

The appetite for outsourcing cyber security services also remains high for those that currently manage it in-house. The majority (67%) of respondents that are currently managing their cyber provision fully in-house will be looking to outsource some, if not all their provision when they next

procure their cyber operations. 30% would move to an end-to-end service provider, 19% would procure specialist expertise in specific areas, and 18% would move to a hybrid solution.

This demonstrates that for those not currently outsourcing, there is still a desire to relinquish more control for improvements, but for this to be effective, providers must resolve the frustrations leading to the disillusionment experienced by current customers.

## Chapter 3

# Mid-size organisations fare the worst

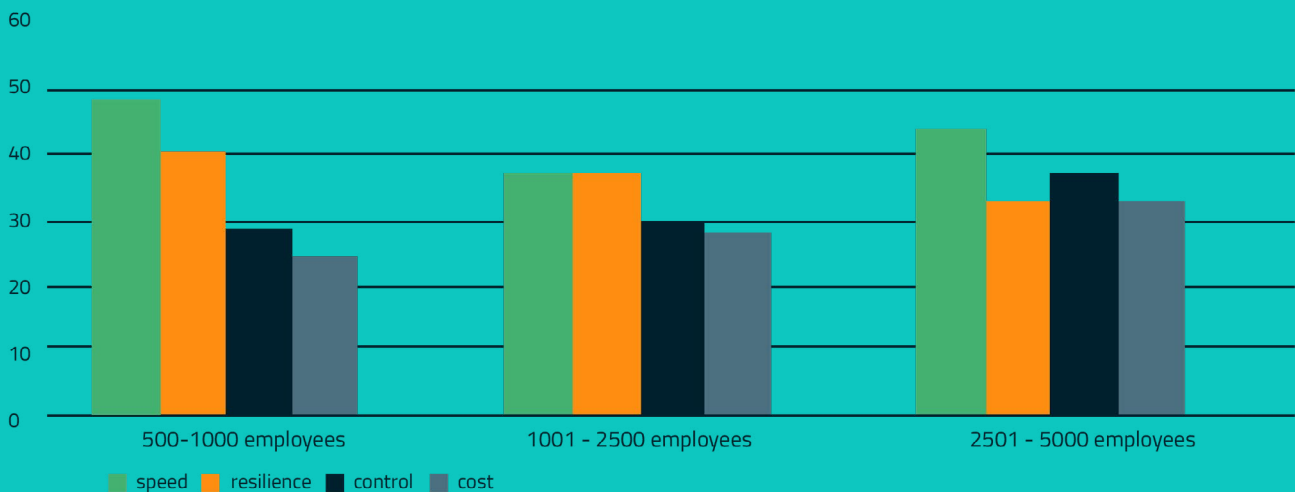
---



**The UK Cyber Security Sectoral Analysis 2023** report indicates that cyber security support for mid-size organisations is continuing to grow. With more players entering the market, there is increasingly more choice for organisations based on the broader range of services available. However, our research finds that the additional choice does not necessarily increase the sophistication of coverage or quality of service delivered by providers. Despite our study showing mid-size

organisations as the most prominent outsourcers (57%), with 29% using SOC-as-a-service, mid-size organisations fare unfavourably in relation to enterprises.

They share similar priorities to those of enterprises, wanting speed (38%), resilience (38%), and control (30%) from their security providers. But interestingly, cost ranked last at 28% which indicates that mid-size organisations are not shy in investing.



## Flexibility and transparency is lacking

Compared with enterprises, mid-size organisations are much less likely to have flexible contracts that can evolve from the original contract scope (62% compared to 46% of enterprises). This is a key omission for organisations in this demographic, with many needing this flexibility to expand or scale. Mid-size organisations are also less likely to have transparent pricing from their provider (66% compared with 44% of enterprises). This means that they are more likely to bear hidden charges than larger enterprises that have more clarity and transparency of their pricing.

**62% mid-size**

organisations are much less likely to have flexible contracts that can evolve from the original contract scope compared to

**46% of enterprises.**



# Specialist expertise

Our study finds that services are less likely to be personalised for mid-size organisations. Organisations are less likely to have client-centric delivery teams (with 57% of mid-sized organisations less likely to have this compared with 50% of enterprises); less likely to benefit from tooling that can be tailored to their specific business needs (with 58% of mid-sized organisations less likely to have this

compared with 50% of enterprises); and less likely to leverage analysts with certifications linked to their tech stack (with 60% of mid-size organisations less likely to have this compared with 44% of enterprises). This means mid-size organisations are ultimately not benefiting from the same degree of specialist expertise and tooling as enterprise organisations, which therefore puts them at a higher risk of compromise.



# Confidence

Unfortunately, mid-size organisations are also less likely to have agreed SLAs and KPIs (with 55% of mid-sized organisations less likely to have this compared with 44% of enterprises). Together this suggests that providers are less accountable to mid-size organisations than to enterprises, meaning that to some extent, there is weaker governance and less clarity of the value being delivered by their service provider.

Perhaps unsurprisingly, the poorer results for mid-size organisations have a knock-on effect on how happy and confident they are with their provider. Mid-size organisations report that they are less confident (59%) than enterprises (52%) in detecting threats. This is perhaps also linked to their lack of confidence in their providers, with 47% of mid-sized organisations reporting underperformance and only 22% of mid-size organisations believing that they are resilient.

## Five fundamentals regardless of company size

With mid-size organisations among the most prominent outsourcers in our study, it is clear they have the most to gain from specialist knowledge and expertise to guide them to best practice. There are several fundamentals that should be delivered by a provider, regardless of organisation size. Here are five key requirements to discuss with your incumbent cyber security provider:



**Frequent testing with alerts when posture falls below baseline.**



**Service evolution that keeps the provider ahead of industry trends.**



**Clear, progressive roadmaps to stay ahead of threat actors.**



**Easily consumable reporting to demonstrate value and justify investment.**



**Clear paths of escalation if the provider is underperforming.**

Chapter 4

# Cyber defence rejuvenation in 2024

---

The findings from our 2024 threat detection research highlight the integral need for the shift in both the service and commercial offerings from cyber security providers. We know that CISO's desire flexible (50%) and rolling (43%) contracts, and transparent pricing (44%). Almost half (43%) also desire stronger client centricity from their delivery with more effective communication and account management. e2e-assure predicts that this shift in CISO priorities will result in five key trends in 2024:



## 1. Providers will need to prove their value

With over half (59%) of those surveyed suggesting that their current outsourced cyber provider is underperforming, it is evident that a critical shift is needed to regain the confidence in CISOs and cyber security decision-makers. At present, in-house teams have stronger governance and more defined KPI's and SLA's, making it easier for CISOs to see the value internal teams are delivering. For outsourcing providers to remain competitive, they must therefore be more accountable in 2024 or risk what our research suggests is a growing trend to bring provisions back in-house or merge as a hybrid model.



## 2. Security teams will relinquish more control to trusted providers

Despite a degree of CISO disappointment, the majority of respondents recognise the limitations of their in-house security teams and are happy to relinquish more control to providers in return for quicker decisions (68%), faster response times (63%) and less reliance on in-house skills (61%). This suggests that in 2024, providers should integrate more closely with internal teams and take on more responsibility. This shift should see providers spearheading cyber defence roadmaps and leading CISOs through the evolving landscape.



## 3. Contracts will be more commercially flexible

CISOs and senior cyber security decision-makers are demanding more from their commercials with both flexible contracts (43%) and transparent pricing (42%) being desirable. This indicates that in 2024, commercial flexibility will play a more integral part in a company's cyber defences, as long fixed contract terms without a clear road map will cause organisations to be left behind as cyber-attack tactics continue to evolve.



## 4. Service and tooling flexibility becomes more of a priority

In line with the shift towards flexible commercials, our research also predicts that service flexibility will be a key deciding factor in contract negotiation in 2024. A common industry trend that is revealing itself is the increased need to scale down technological investment and consolidate tooling to better enhance cyber resilience. Security teams will therefore become more resistant to one of their biggest frustrations – the continuous need to bolt on new services to meet their security needs (27%). With CISOs and cyber security decision-makers prioritising the ability to amalgamate tech stacks (43% of those surveyed stated tooling that can tailor services to their environment is desirable), it will be the providers that are more agile in their ability to integrate into multiple vendor toolsets that will present themselves as most attractive.



## 5. Quality cyber defence will become more accessible

Our research identified multiple barriers for mid-size organisations, from being less likely to have flexible commercials and specialist expertise to agreed SLAs. These findings therefore suggest that the mid-market will rightly start demanding similar commercial flexibility and service offerings to that of enterprise organisations to enable them to feel more confident in their cyber defence agility. With supply chain attacks on the rise, it could be argued that mid-market companies are in equal need of enterprise-level protection and so we will start to see a growing trend over coming years where higher quality cyber defence becomes more accessible to mid-size organisations.

The desired shifts from CISOs and senior security decision-makers underscores the importance of a holistic and agile cyber security strategy. The demand for specialist expertise is still there and our research suggests that boutique cyber

defence offerings that are more agile due to size and offer a more client-centric focus, provide greater clarity, precision and control for security teams within mid-sized organisations.

# Proactively disrupting attackers to safeguard your business

e2e-assure gives you the advantage in protecting your business against cyber threats. We abstract away all unnecessary complexity from the communication channels and empower your teams with clear, understandable and actionable knowledge.

Our drive for innovation is focussed on continually reducing the friction, time and cost of protecting your business against cyber criminals. We are meticulous in applying cutting edge technology capabilities to solve real business problems and ensuring that only high value signals gain attention and distracting noise is eliminated.

We give you back time, budget and headspace to reflect and plan security improvements in a careful and considered manner.

## Monthly Threat Intelligence Summaries

Found this report helpful? Sign up to our monthly Threat Intelligence Summary Newsletters to stay up to date with the latest development in cyber threat tactics. You'll be among the first to know about new cyber threats and how to protect your business against them. You'll also receive exclusive content, such as whitepapers and case studies, that can help you stay informed about best practices for cyber security.

Don't miss out on this valuable resource – sign up for our threat summaries today and stay one step ahead of cyber threats.

[Sign up here](#)

In this research, enterprises are defined as companies with 2,501 – 5,000 employees and mid-size businesses are defined as companies with 1,001 – 2,500 employees.