A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

CYBERSECURITY TRENDS AND PRIORITIES REPORT AT GISEC 2025

A PRIORITIES REPORTS, EVENTS & WEBINARS Report

in collaboration with Recorded Future®

A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

CONTENTS

A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

INTRODUCTION

The Middle East – a region rapidly embracing Digital Transformation – finds itself at the forefront of a dynamic and challenging cybersecurity landscape. From burgeoning e-commerce platforms to critical infrastructure deployments, the region's increasing reliance on digital technologies has simultaneously amplified its exposure to sophisticated cyberthreats.

This *Cybersecurity Trends and Priorities Report at GISEC 2025* provides a comprehensive overview of the critical cybersecurity challenges and evolving priorities faced by organisations across the Middle East. Driven by geopolitical tensions, the accelerated adoption of cloud services and the proliferation of advanced threats like ransomware and state-sponsored attacks, organisations are having to navigate an unprecedented wave of risks.

"The results emphasise the dynamic and multi-faceted nature of modern cybersecurity management, demanding adaptable and comprehensive strategies."

The report delves into the key factors driving cybersecurity investment, exploring how regional entities are strategically allocating resources to bolster their defences. Furthermore, we examine the prioritisation of advanced technologies, such as AI-powered threat detection and Zero Trust architectures, as organisations strive to build resilient and future-proof security postures. The analysis aims to provide insight into the strategic approaches being adopted to secure the digital future of the region.

METHODOLOGY

We surveyed 150 senior IT security decision-makers from a diverse set of industries across the GCC region. Job titles included CISOs, CSOs, Director of Cybersecurity and Head of Cybersecurity.

A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

FOREWORD

EMAD FARAJ
SENIOR DIRECTOR, META AT RECORDED FUTURE

Every day across the Middle East, security teams face the impossible task of sorting through millions of alerts daily, each potentially critical. Somewhere within this noise are the signals that truly matter – the ones they cannot afford to miss. But what's happening in the Middle East today represents something unique. The META region isn't just adapting to digital transformation – it's embracing it at an unprecedented pace, creating both extraordinary opportunity and escalating risk.

At Recorded Future, our mission is clear: securing our world with intelligence. This *Cybersecurity Trends and Priorities Report* reveals a security environment where comprehensive threat visibility has become essential for organisations operating in the Middle East.

The Middle East's accelerated adoption of digital technologies has created an expanded attack surface that sophisticated threat actors are actively targeting. This environment demands precision intelligence, not generic information. At Recorded Future, we've measured our impact: our data shows 86% of organisations using our intelligence are now taking a proactive approach rather than merely reacting to threats. They're seeing benefits that extend far beyond security operations – 64% report a fundamentally better understanding of their threat landscape, while detection and remediation times have decreased by nearly half (46%).

Yet many security teams continue to face an impossible daily challenge: sorting through millions of alerts to find the signals that truly matter. This is where intelligence that delivers precision becomes transformative. By connecting dots across internal telemetry and external threats through our AI-driven Intelligence Graph®, security teams gain the context they need to prioritize what matters most to their business.

As the region embraces advanced technologies like AI-powered threat detection and zero trust architectures, we're witnessing a profound shift in how organisations approach security. It's no longer about building higher walls – it's about seeing threats first and acting when it matters most. This evolution reflects a deeper understanding that in today's landscape, generic intelligence isn't intelligence at all.

The insights in this report offer not just a window into the threat landscape, but a roadmap for building resilience in a region that's rapidly redefining what's possible.

A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

SUMMARY OF FINDINGS

Around a quarter of respondents cited budget constraints as the biggest cybersecurity challenge while one fifth highlighted evolving threats and integration issues.

Two key challenges dominate cybersecurity management: nearly one-fifth of respondents pointed to regulatory burdens, while a substantial number highlighted the difficulty of keeping pace with rapid technological changes.

Nearly a third of those surveyed claim 'Excellent' and a further quarter 'Good' when rating their organisation's overall cybersecurity posture.

Referring to strategies for dealing with ransomware attacks, almost a third of those surveyed prioritise preventative measures and backups; a positive sign.

When addressing common cybersecurity mistakes, nearly a third of respondents cite phishing link clicks as the primary issue, with a further quarter noting weak password practices.

When exploring factors that contribute to individual effectiveness of managing cybersecurity threats, almost one-sixth emphasise both clear communication and proactive threat intelligence.

Roughly a third believe proactive threat detection and prevention is the greatest advantage of using AI in cybersecurity.

Over half of the respondents are actively leveraging AI/ML, highlighting a growing recognition of its value in enhancing cybersecurity capabilities.

When considering cybersecurity priorities for the next 12 months, almost a third will prioritise endpoint security, with a further quarter focusing on advanced threat detection.

A slight majority of organisations plan to increase their threat intelligence investment in 2025.

Over half of those surveyed reported increased cybersecurity budgets for 2025.

Nearly a third of respondents cite the emerging threat landscape as the primary influence driving cybersecurity investment decision.

Threat Intelligence Platforms (TIP), Security Orchestration, Automation and Response (SOAR) and Identity and Access Management are the tools that organisations are most commonly integrating with intelligence tools.

When considering technologies expected to shape the future of cybersecurity, nearly a third anticipate Zero Trust architecture's dominance, with a quarter highlighting Quantum Computing.

Regarding the operational benefits provided by threat intelligence, almost a quarter identify improved threat analysis and faster incident response as primary benefits.

When consuming threat intelligence, the findings revealed equal results – both nearing a quarter – when relying upon automated feeds and commercial reports.

A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

PART 1

CYBERSECURITY PREPAREDNESS

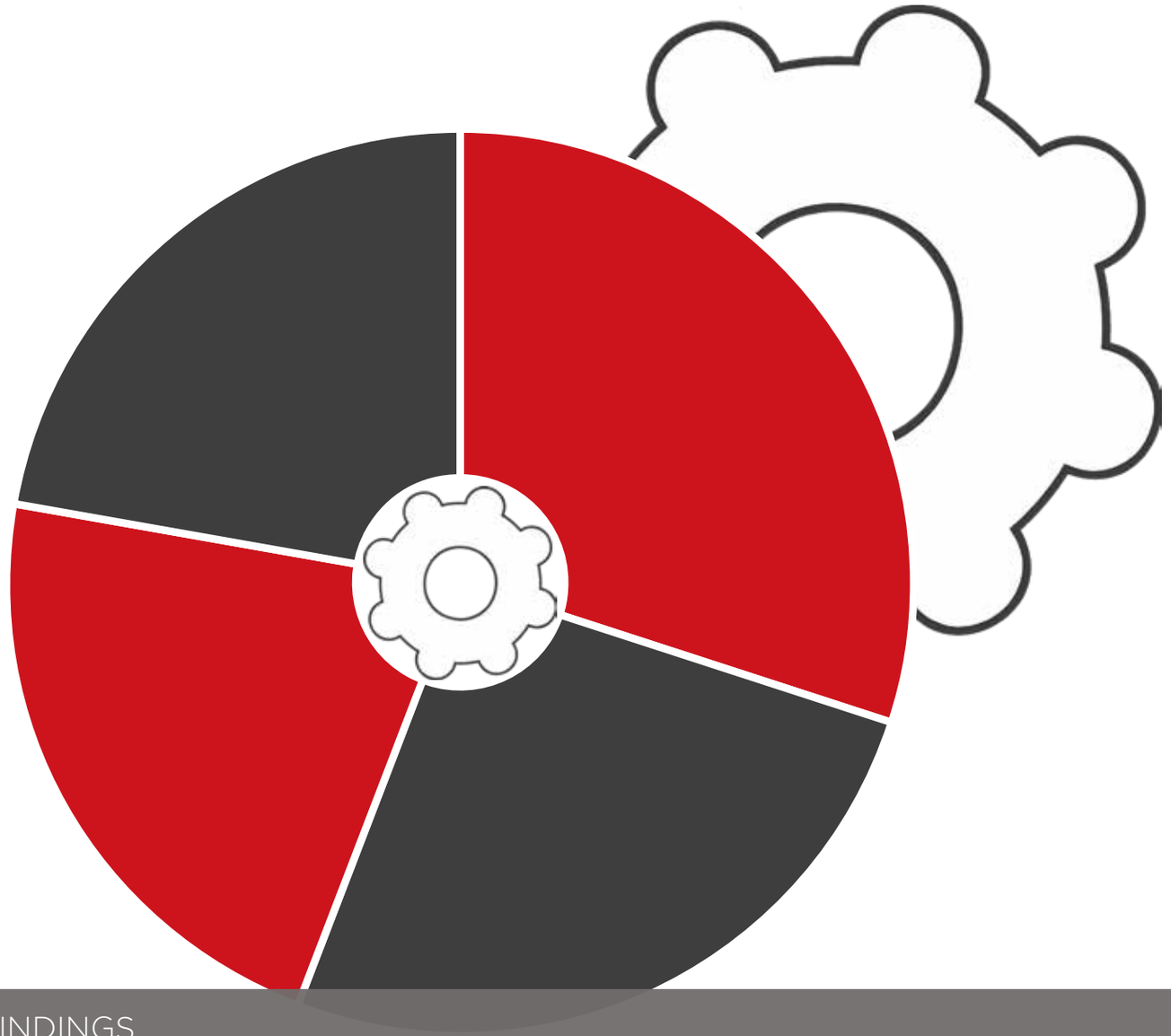
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 1

How would you rate your organisation's overall cybersecurity posture?



Excellent	30%
Good	26%
Fair	22%
Poor	22%

KEY FINDINGS

We notice a concerning lack of decisive confidence in these findings. Nearly a third of those surveyed claim 'Excellent' and a further quarter of those people 'Good', suggesting a veneer of security. The equal turnout of 'Fair' and 'Poor' indicates a worrying underlying vulnerability. This necessitates a targeted, culturally nuanced approach to security assessment, particularly pertinent in the evolving digital landscape of the Middle East where regional threats and regulatory frameworks demand specialised expertise.

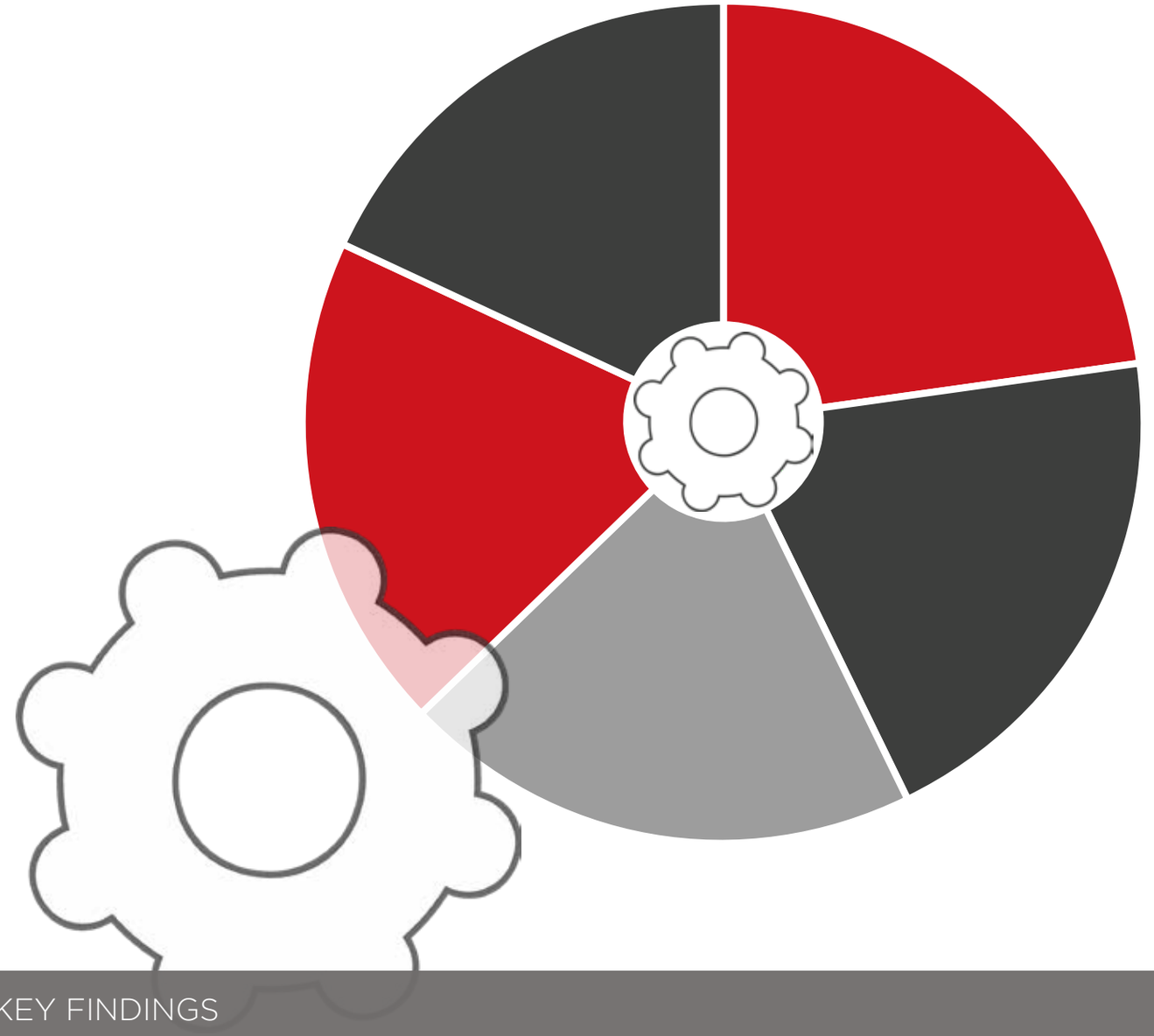
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 2

What are the biggest cybersecurity challenges your organisation faces today? Select two.



Budget constraints	23%
Evolving and sophisticated threats	20%
Integration of security tools and systems	20%
Lack of skilled personnel	19%
Limited awareness or training among employees	18%

KEY FINDINGS

The responses highlight a cluster of tightly packed challenges, indicating a multi-faceted problem. Roughly a quarter cited budget constraints, closely followed by a fifth identifying both evolving threats and integration issues. This suggests organisations grapple with both resource limitations and the technical complexities of modern cybersecurity, revealing a need for strategic, resource-efficient solutions

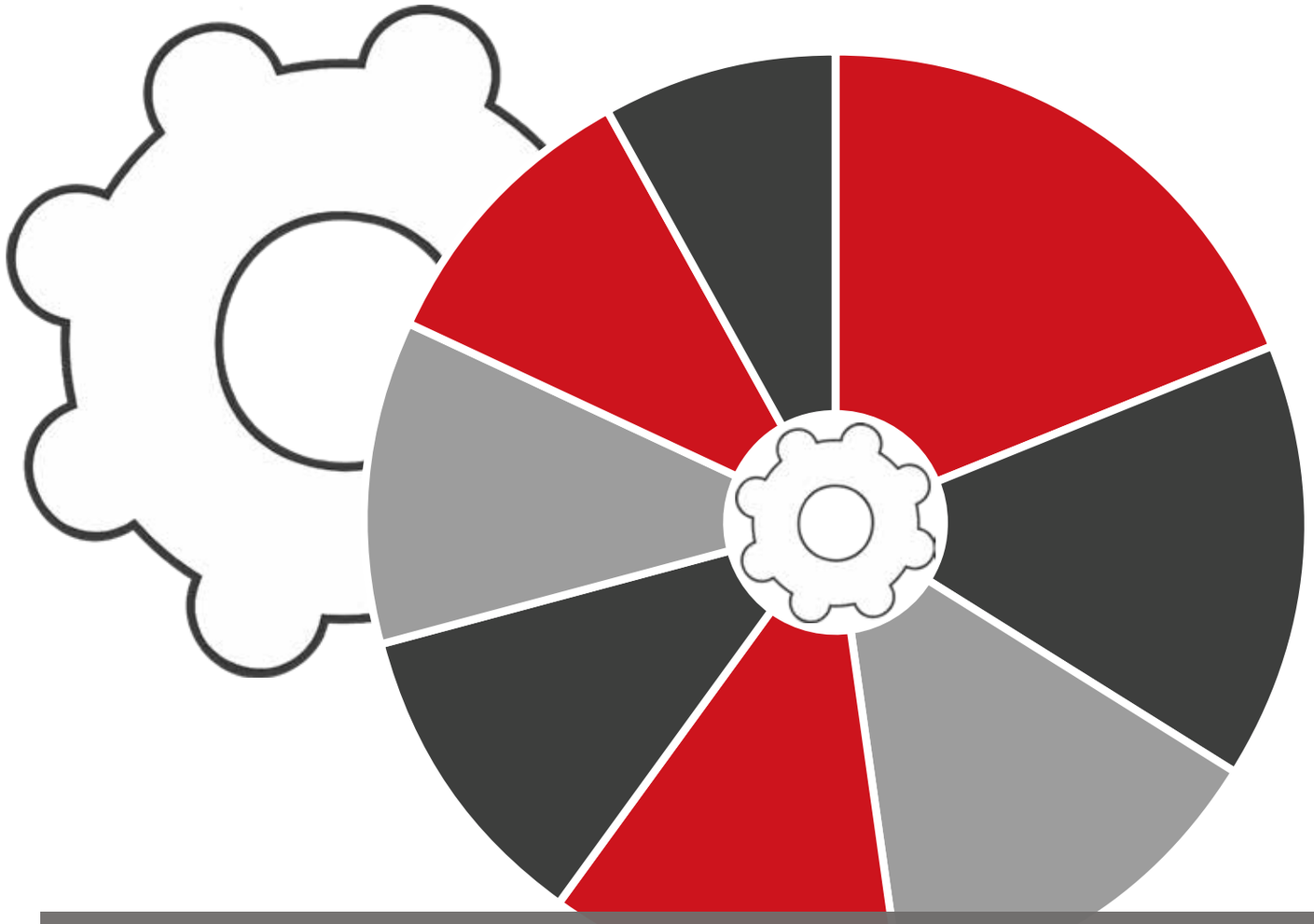
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 3

Which factors contribute most to the complexity of managing cybersecurity in your organisation? Select up to three.



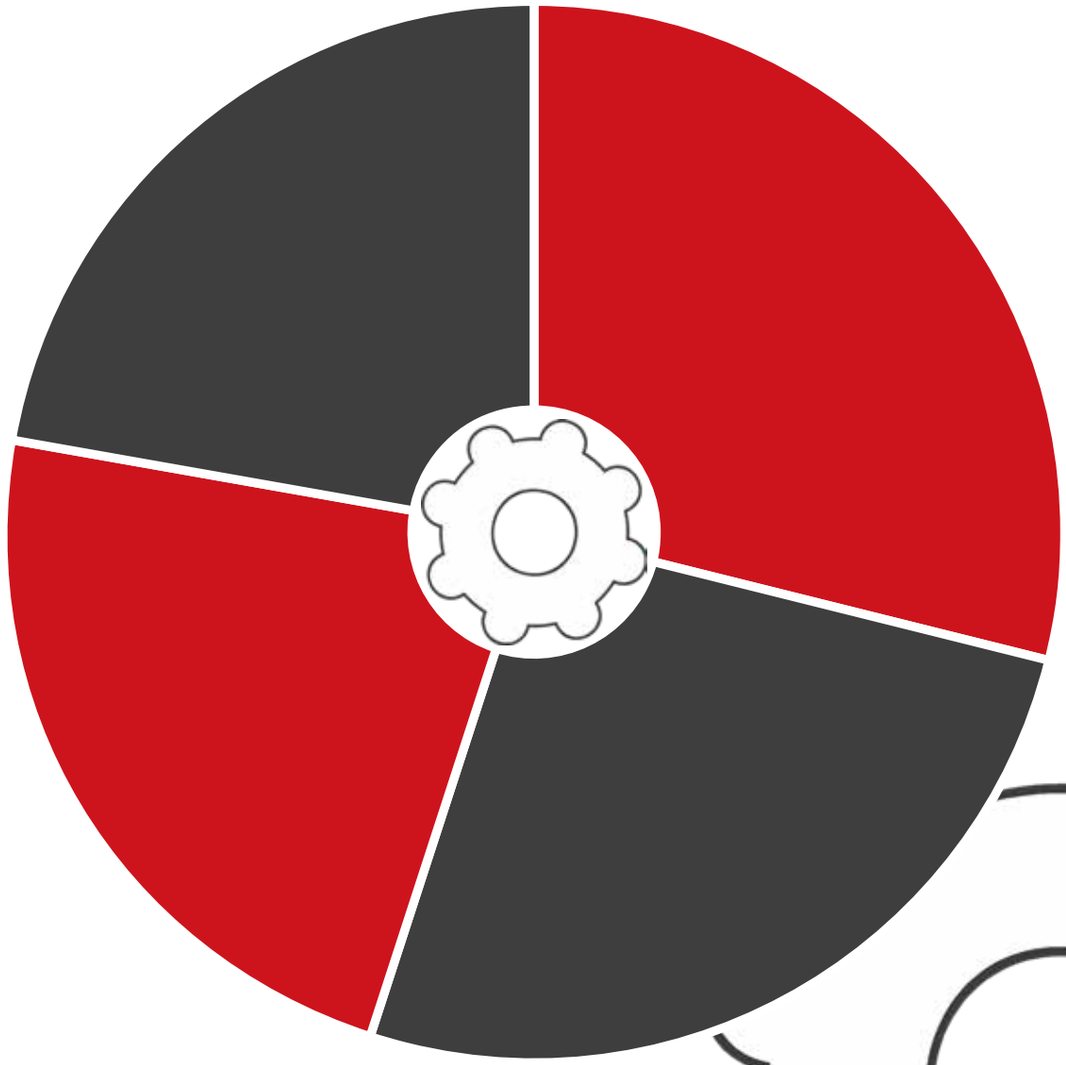
Regulations/legislation	19%
Rapidly evolving technology landscape	15%
Increasing sophistication of cyberthreats	14%
Managing technology stack	12%
Managing cyberawareness/training across wider organisation	11%
Budget constraints	11%
Obtaining support from C-suite for initiatives	10%
Lack of skilled cybersecurity personnel	8%

KEY FINDINGS

The data reveals a confluence of contributing factors, demonstrating a nuanced challenge. Nearly one-fifth (19%) cite regulatory burdens, with a significant proportion (15%) highlighting the rapid technological evolution. The increasing sophistication of threats further exacerbates this complexity. The results emphasise the dynamic and multi-faceted nature of modern cybersecurity management, demanding adaptable and comprehensive strategies.

QUESTION 4

How often does your organisation conduct cybersecurity awareness training for employees?



Monthly or more	29%
Quarterly	26%
Annually	23%
Rarely or never	22%

KEY FINDINGS

The results demonstrate a near-even distribution across training intervals, indicating a varied approach. Roughly a third of organisations conduct training on a monthly basis or even more frequently, while 26% do so quarterly. However, a significant proportion of respondents – nearly half – train annually or less, revealing a potential vulnerability. This suggests a need for more consistent and frequent awareness training to mitigate and prevent human risk.

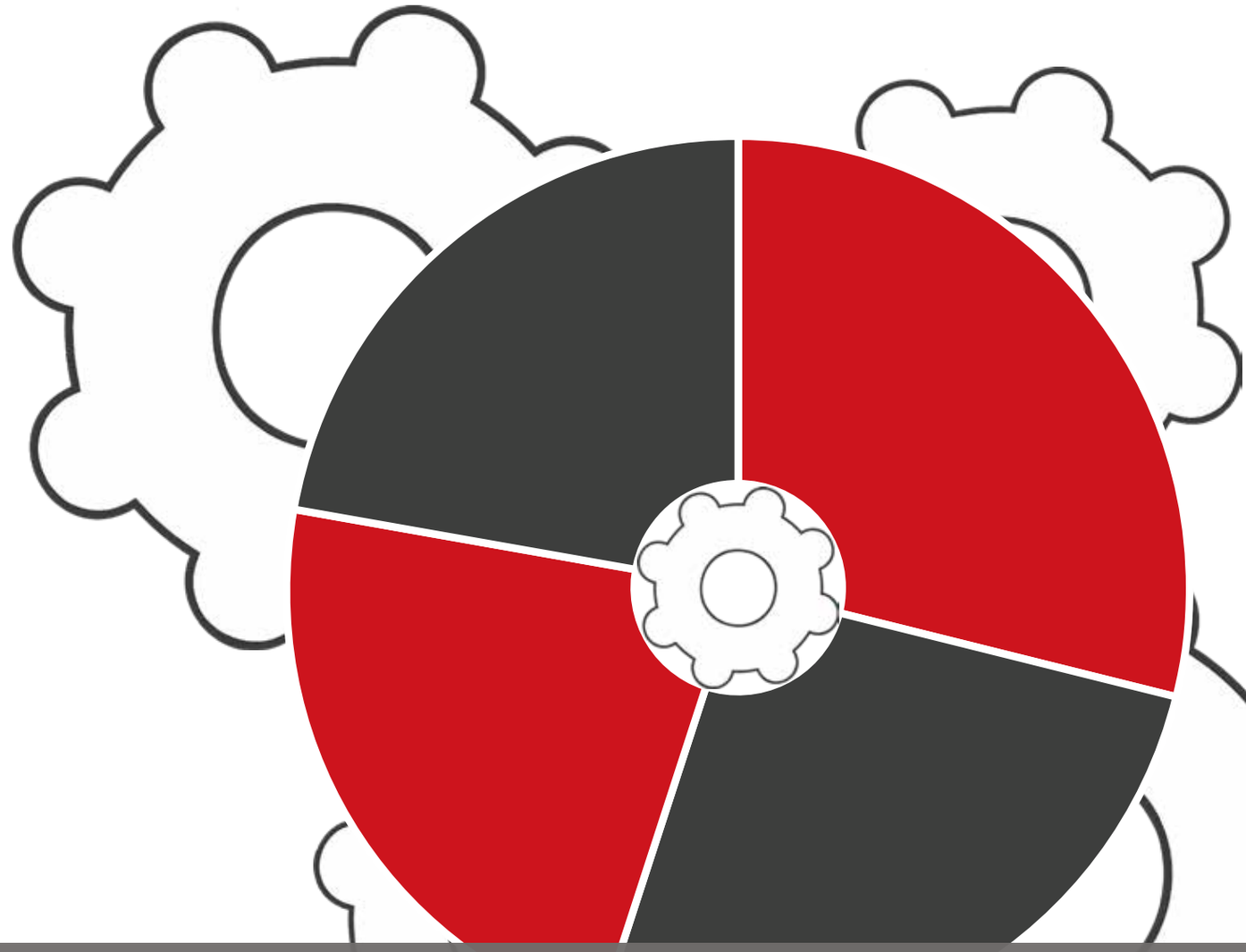
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 5

What is the most common cybersecurity mistake employees make?



Clicking on phishing links or emails	29%
Using weak passwords or reusing them	26%
Failing to report suspicious activity	23%
Sharing sensitive information without proper verification	22%

KEY FINDINGS

The findings reveal a tight clustering of common errors, highlighting persistent human vulnerabilities. Nearly a third (29%) cite phishing link clicks as the primary issue, with a further quarter (26%) noting weak password practices. A significant proportion – almost half – identify a failure in reporting suspicious activity as well as the sharing of improper information as other major concerns. The data underscores the critical need for targeted employee education and robust cybersecurity protocols.

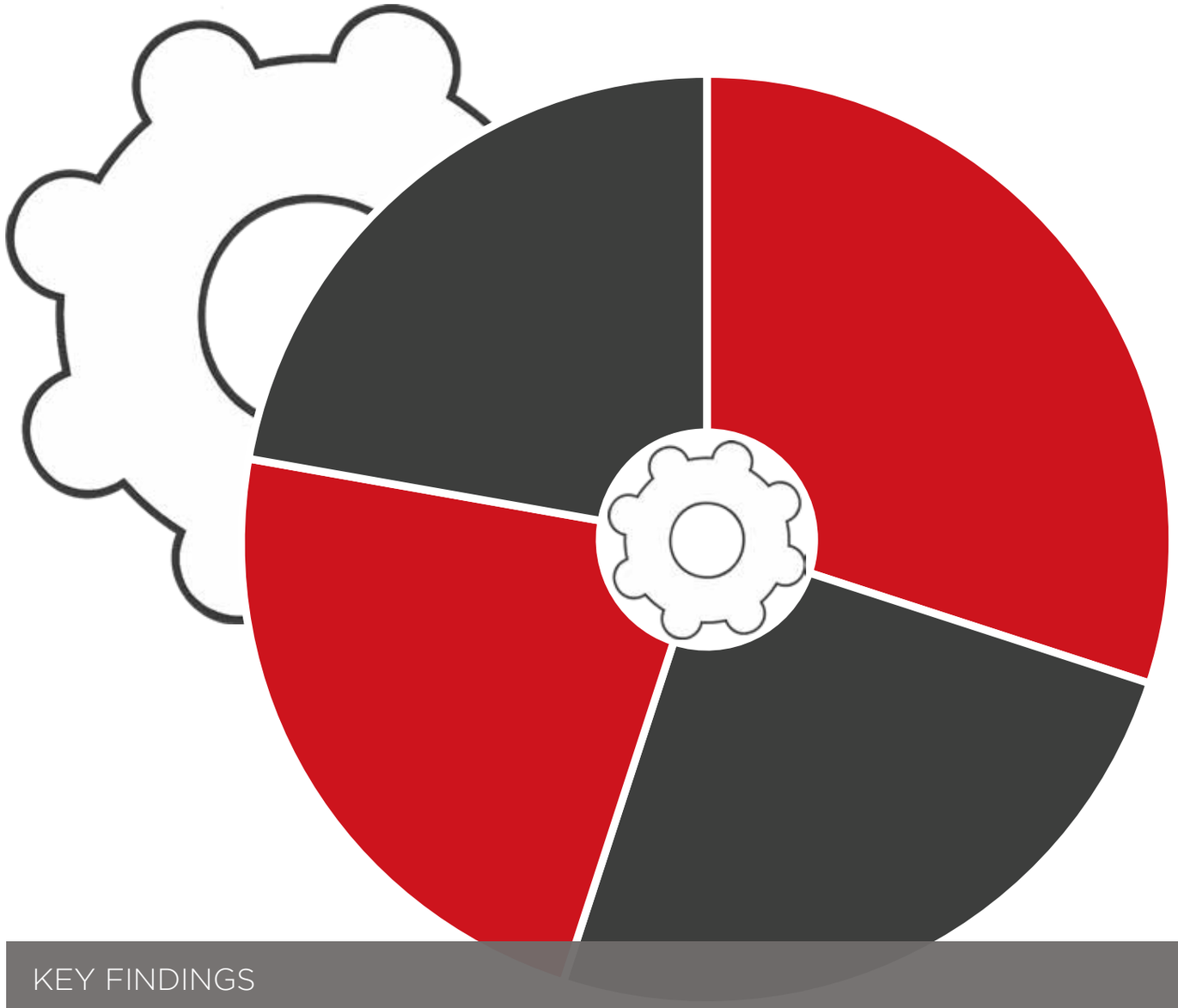
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 6

What is your organisation's strategy for dealing with ransomware attacks?



Preventative measures and regular backups	30%
Incident response plan and negotiations	25%
Paying the ransom to recover data	23%
No formal strategy in place	22%

KEY FINDINGS

Regarding strategies for dealing with ransomware attacks, a large sum (30%) of those surveyed prioritise preventative measures and regular backups; a positive result. However, the findings show that a quarter (25%) rely on incident response and negotiations, while 23% admit to paying ransoms. Alarmingly, a significant portion (22%) lack a formal strategy. This highlights a critical and urgent need for robust, proactive ransomware defence and incident management protocols.

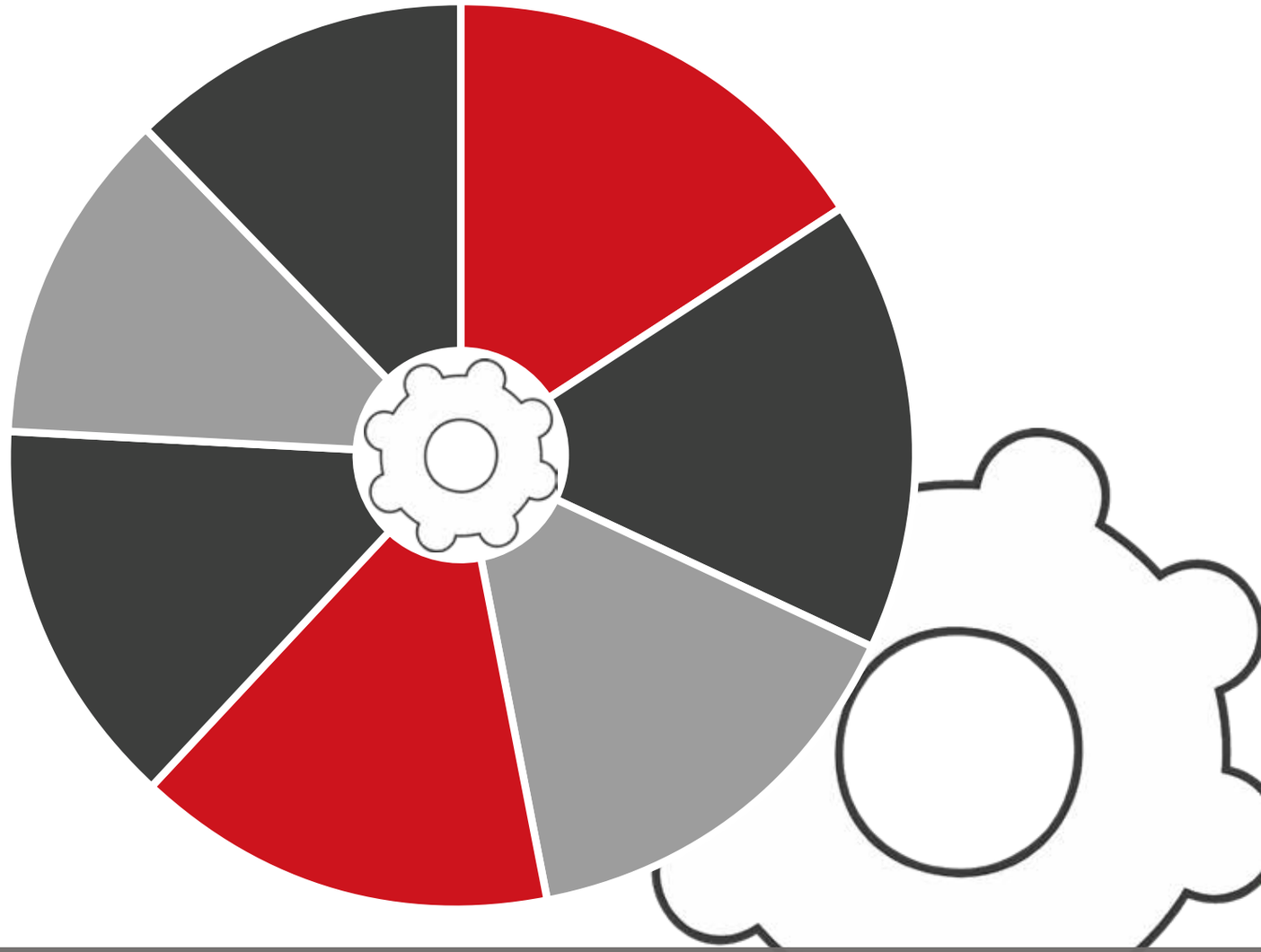
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 7

What key factors do you believe contribute to your individual effectiveness of managing cybersecurity threats? Select up to three.



Clear communication skills	16%
Proactive threat intelligence monitoring	16%
Collaborative approach	15%
Regular training	15%
Strong technical expertise	14%
Strategic planning	12%
Strong relationships with vendors/partners	12%

KEY FINDINGS

The responses reveal a collection of closely ranked contributing factors, demonstrating a holistic view of necessary skills. A total of 16% of respondents emphasise both clear communication and proactive threat intelligence as being significant. A good proportion – with a combined total of 44% – highlight collaboration, training and technical expertise as key contributors. The data indicates that effective cybersecurity management relies on a blend of technical proficiency and soft skills, underlining the importance of a well-rounded approach.

A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

PART 2

AI IN CYBERSECURITY

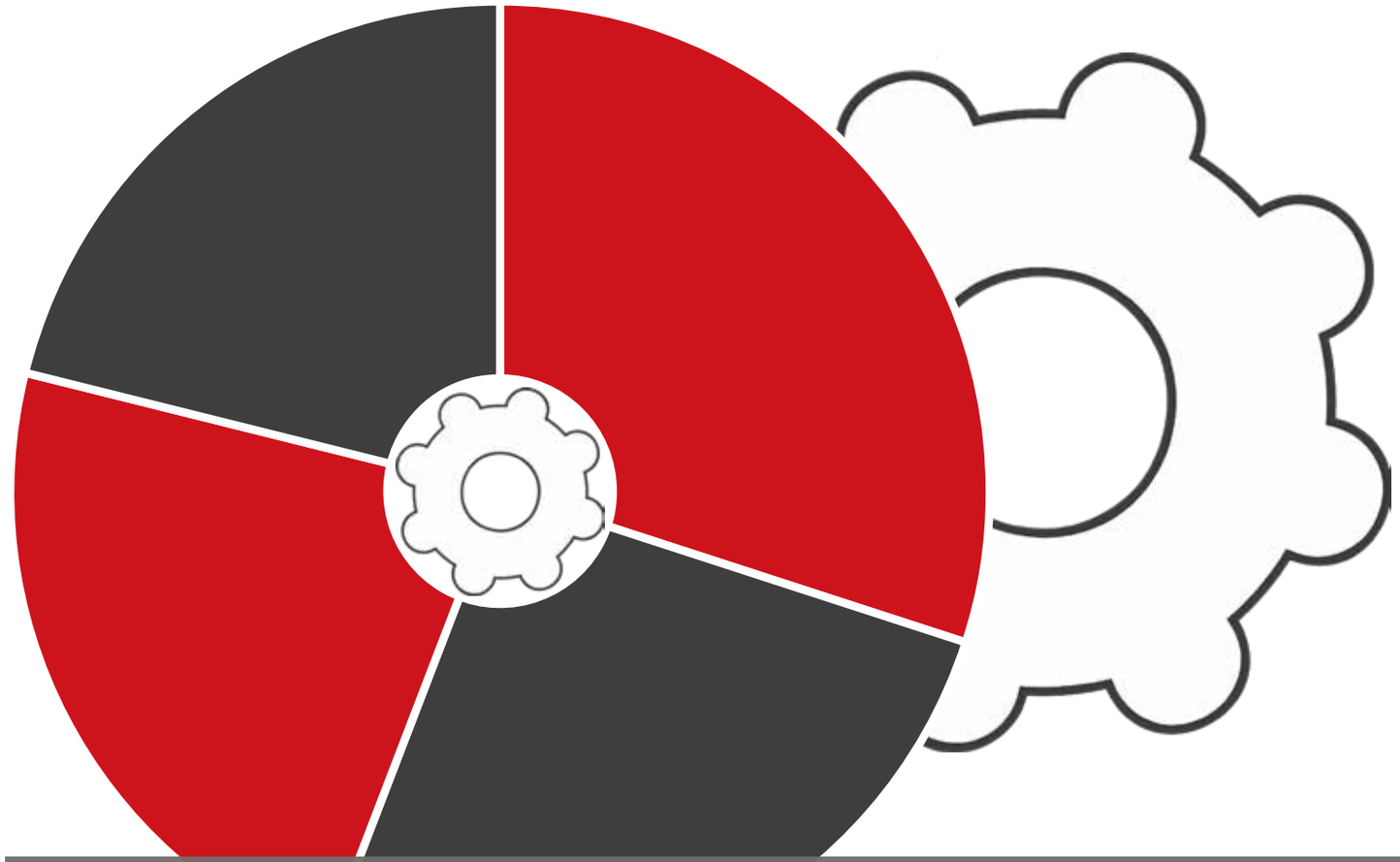
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 8

Is your organisation currently using AI or Machine Learning tools to enhance cybersecurity?



Yes, extensively	30%
Yes, in limited applications	26%
No and we have no plans to	23%
No, but we plan to in the near future	21%

KEY FINDINGS

AI in the cybersecurity sector has been referred to as a ‘double-edged sword’. While it offers significant advantages for defenders – particularly through proactive monitoring, automation and augmenting the widely reported skills gap – it has also been used to launch sophisticated attacks with worrying ease. Despite this, many organisations are leveraging AI to stay ahead of evolving threats, with more than half of respondents already using AI or Machine Learning tools to enhance their cybersecurity. For almost one-third, this technology is being used ‘extensively’, while 26% are using it in more limited applications. A further 21% plan to use AI tools in the near future, while the remaining 23% have no plans to. This may highlight the varying maturity levels of AI in cybersecurity across the region and, as this technology becomes better understood, may be subject to change.

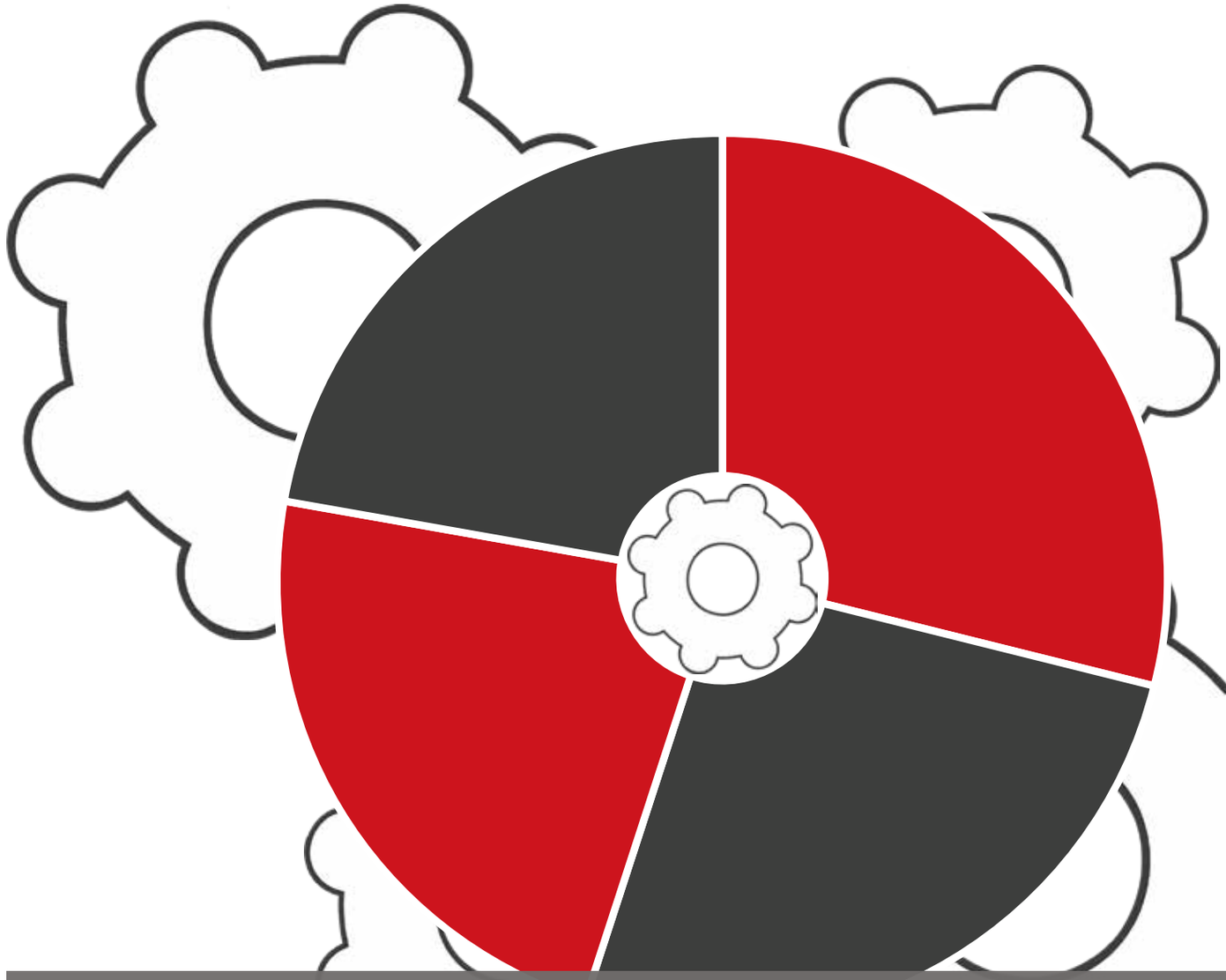
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 9

What do you see as the greatest advantage of using AI in cybersecurity? Select two.



Proactive threat detection and prevention	29%
Improved efficiency in monitoring and incident response	26%
Reduced reliance on human resources	23%
Enhanced accuracy in identifying anomalies	22%

KEY FINDINGS

The greatest advantage of using AI in cybersecurity, according to our respondents, is for proactive threat detection and prevention, with 29% of the vote. This is closely followed by improved efficiency in monitoring and incident response (26%). This result demonstrates how CISOs in the region perceive AI to be most impactful, enabling a more proactive cybersecurity posture. It will also support human workforces by automating many traditionally labour-intensive elements of the role.

A Lynchpin Media BRAND

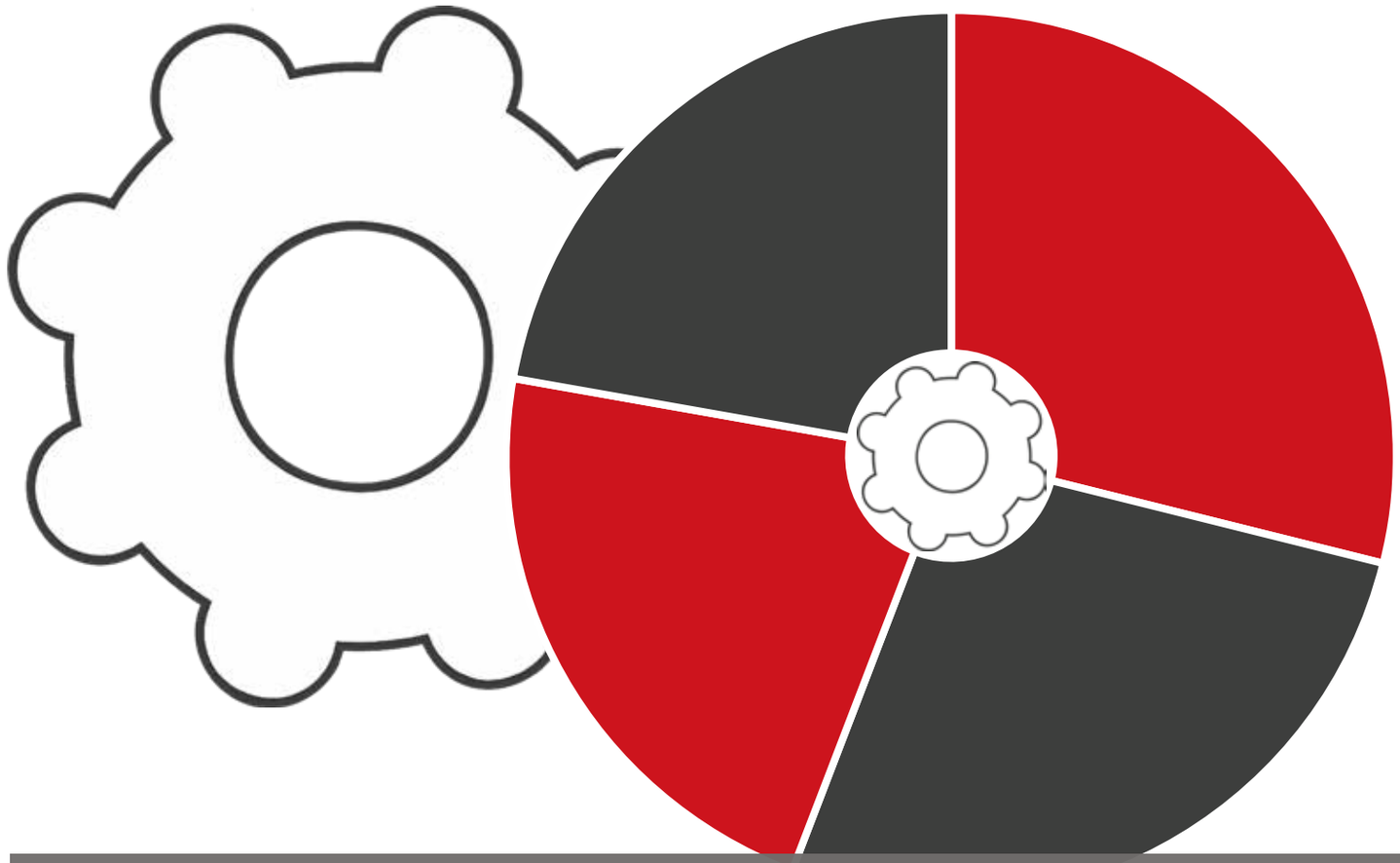
CIO PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

FUTURE CYBERSECURITY PRIORITIES

QUESTION 10

What are your organisation's top cybersecurity priorities for the next 12 months? Select two.



Strengthening endpoint security	29%
Implementing advanced threat detection systems	27%
Improving employee training and awareness	22%
Enhancing data protection and privacy measures	22%

KEY FINDINGS

CISOs across the GCC are managing a plethora of diverse, competing challenges and this is reflected in the responses which were split across several different areas. With a slightly higher percentage of the vote (29%), strengthening endpoint security is the top priority for the year ahead, followed by implementing advanced threat detection systems (27%). These results highlight a clear focus on securing access points and devices – potentially driven by an increasingly remote workforce and sophisticated attacks on the endpoint, as well as the need for proactive threat detection. Organisations also recognise the need to address employee training and awareness and enhancing data protection and privacy measures, with both receiving 22% of the vote. The findings demonstrate the need to balance 'people and processes' to ensure a strong overall cybersecurity strategy.

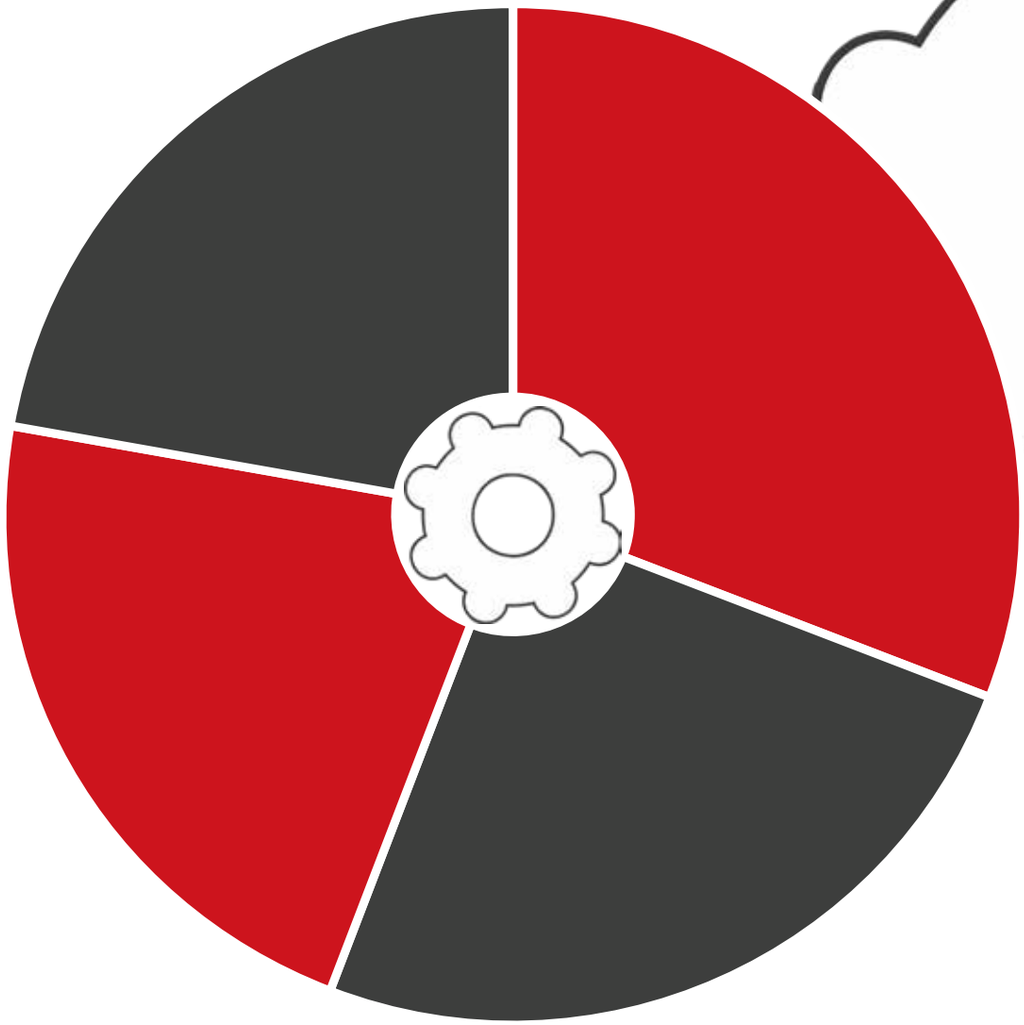
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 11

Compared to 2024, how has your budget for cybersecurity changed for 2025?



The budget has increased by more than 10%	31%
The budget has increased by less than 10%	25%
There has been no change – the budget has remained the same	22%
The budget has decreased by more than 10%	22%

KEY FINDINGS

A significant number of organisations in the GCC are either maintaining or reducing their budgets, according to our research. In fact, more than 55% of respondents reported an overall boost to budget for the year ahead – 31% said this was by more than 10%, while for 25% there has been a slightly lower increase of less than 10%. However, 22% reported a budget that has decreased by more than 10% in 2025 and 22% said there had been no change.

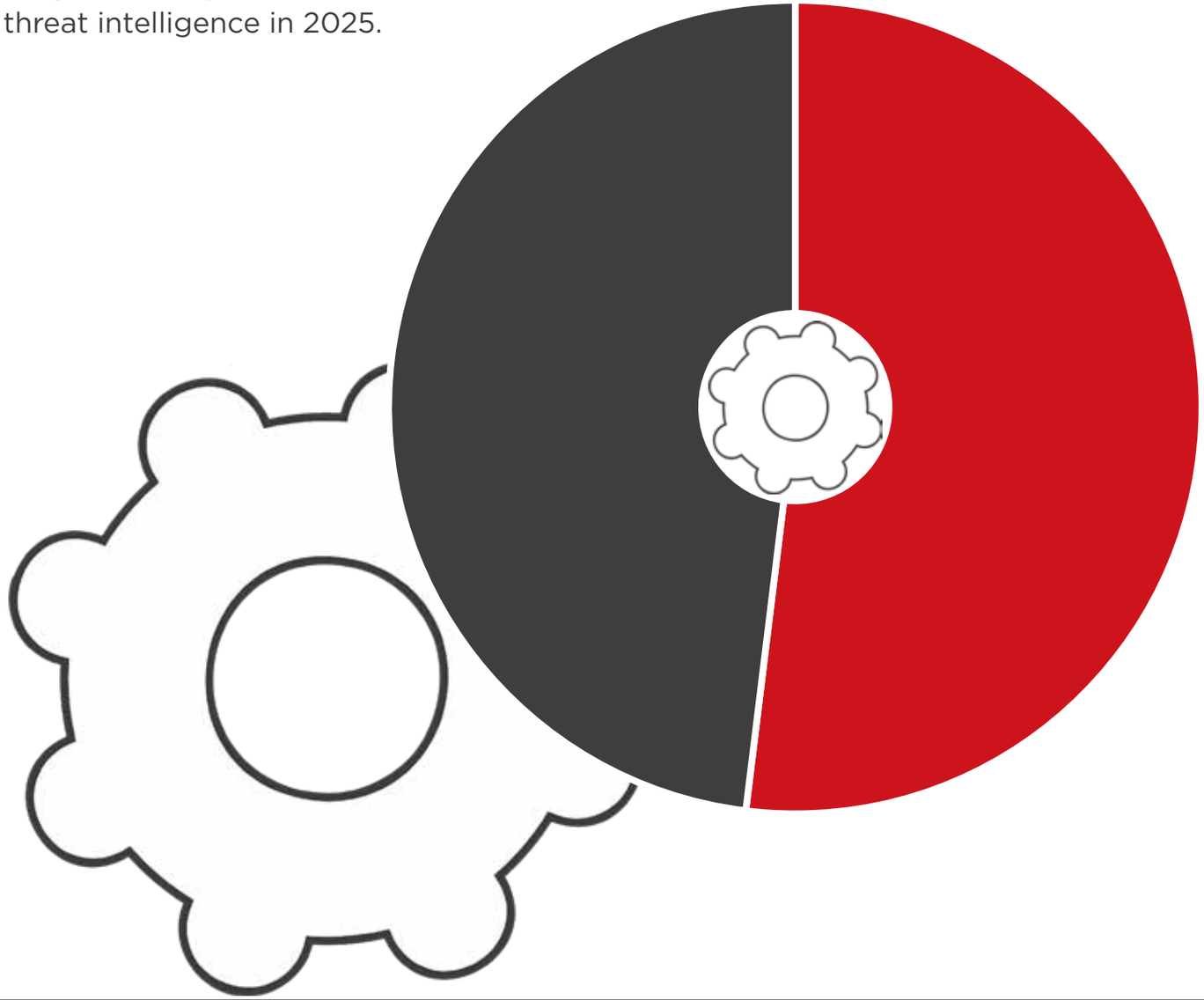
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 12

My organisation plans to invest more in threat intelligence in 2025.



Yes	52%
No	48%

KEY FINDINGS

Just over half (52%) of CISOs plan to increase investment in threat intelligence in 2025 – indicative of the value seen in enhancing threat intelligence capabilities. With cyberthreats continuing to grow in complexity, the data shows that organisations understand the importance of taking a proactive approach to staying ahead of malicious actors. In contrast, 48% of respondents are not planning to boost their threat intelligence capabilities in the coming year. This could be due to budget constraints or a shift in focus, prioritising other areas within cybersecurity.

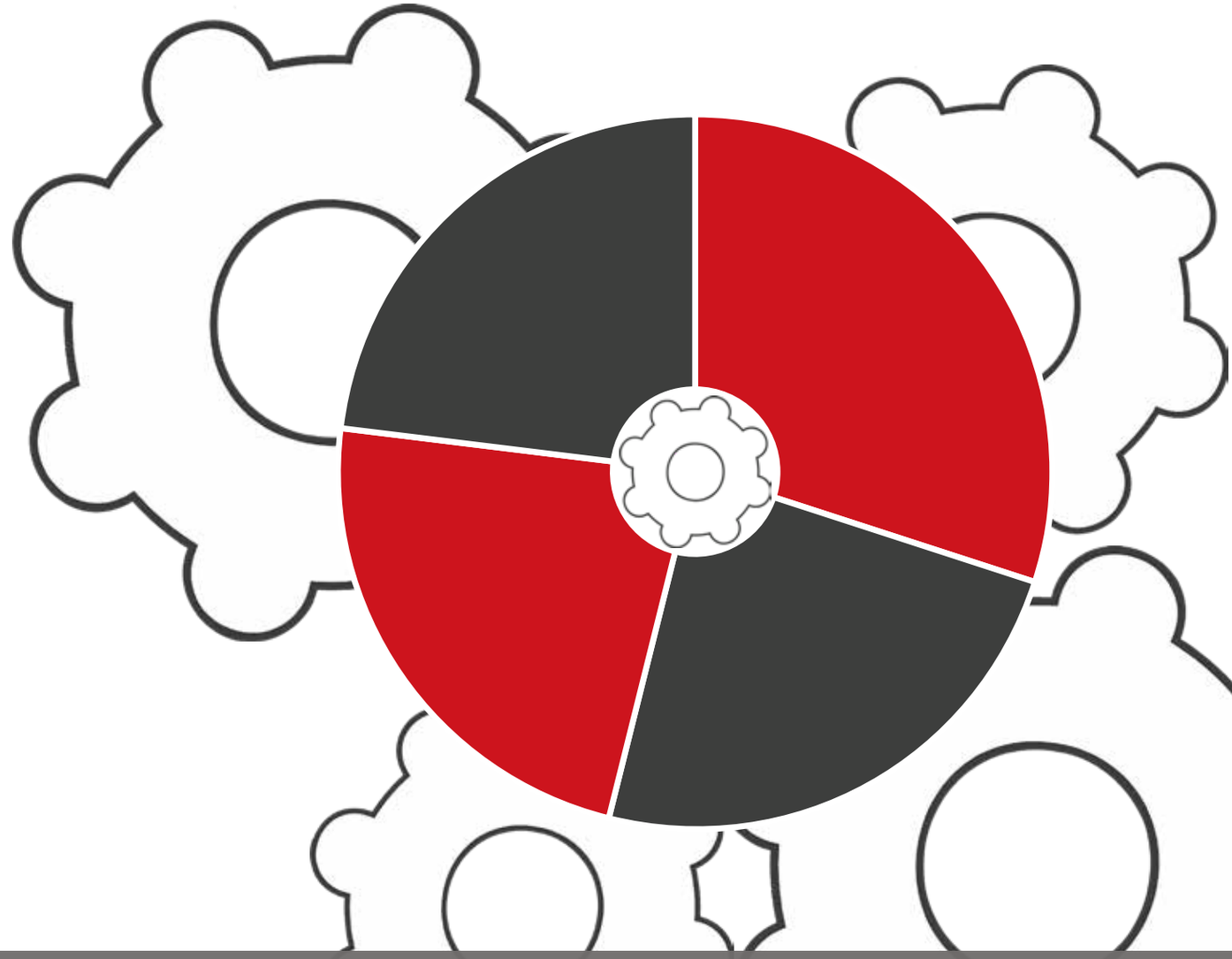
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 13

What emerging technologies do you believe will shape the future of cybersecurity? Select two.



Zero Trust architecture	30%
Quantum Computing	24%
Artificial Intelligence and Machine Learning	23%
Blockchain	23%

KEY FINDINGS

While respondents were interested in several emerging technologies, Zero Trust architecture was selected by almost one-third as being most impactful for the cybersecurity sector looking ahead. This has grown increasingly popular in recent times, as organisations have shifted away from a traditional perimeter-based security model, particularly with remote – or at least hybrid – working now the norm. Quantum Computing is also a key focus area, possibly due to its potential to impact encryption.

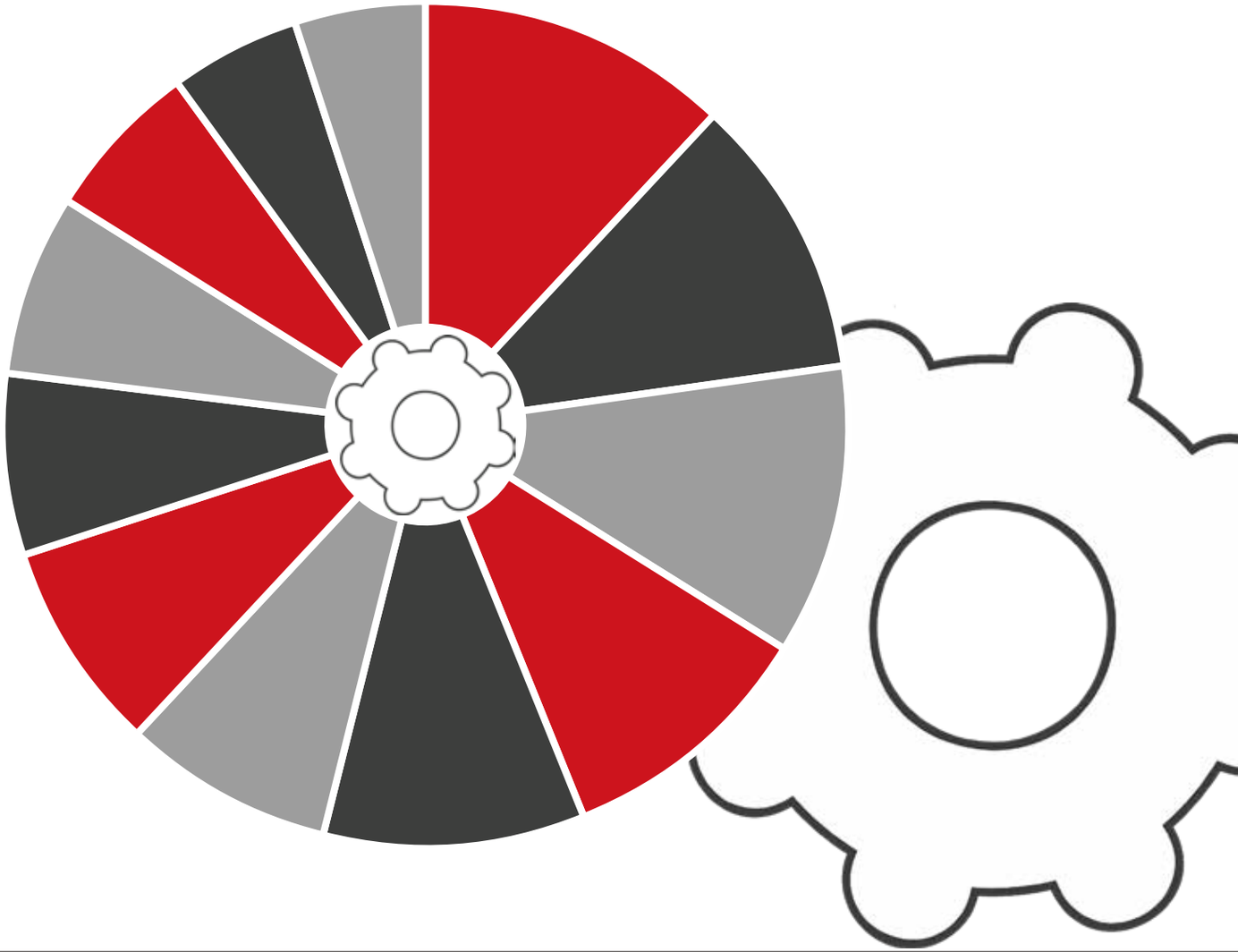
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 14

What tools do you currently integrate intelligence with or plan to integrate with in the next 12 months? Select all that apply.



TIP	12%
SOAR	11%
Identity and Access Management	11%
SIEM	10%
Network Detection	10%
Email Security	8%
Governance, Risk and Compliance	8%
Ticketing	7%
None	7%
Incident Response	6%
EDR/XDR	5%
Cloud Security	5%

KEY FINDINGS

Threat Intelligence Platforms (TIP) (12%), Security Orchestration, Automation and Response (SOAR) (11%) and Identity and Access Management are the tools organisations are most commonly integrating with intelligence tools. This reiterates the value that security teams are placing on automating and enhancing threat detection, response and intelligence sharing. A total of 7% of respondents do not integrate intelligence tools at all, which could point to budget constraints, lack of expertise, or reliance on other security strategies.

A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

PART 3

SECURITY MEASURES AND INVESTMENTS

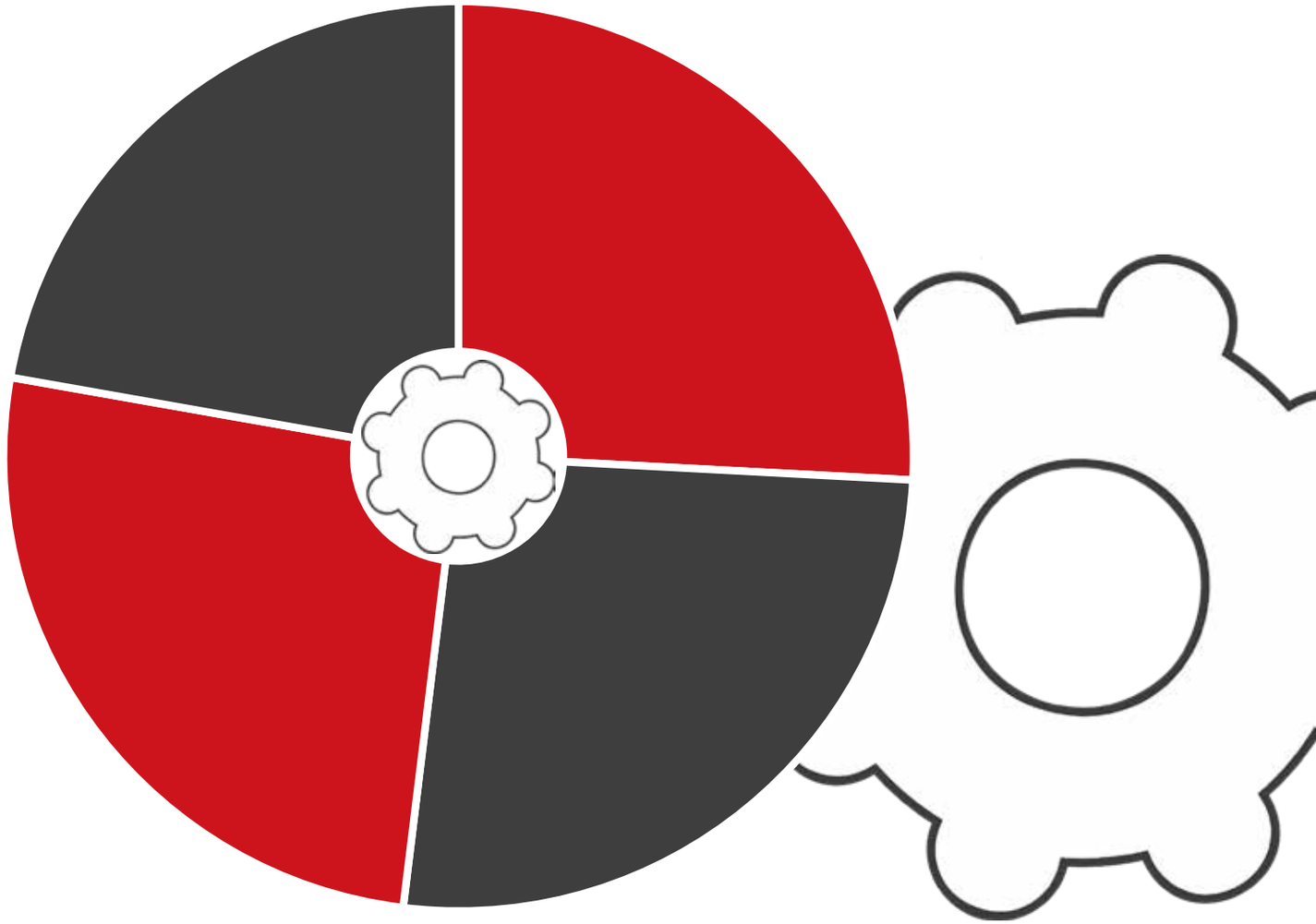
A Lynchpin Media BRAND

PRIORITIES REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 15

Which two security measures have been most effective in protecting your organisation?



Endpoint detection and response	26%
Network segmentation	26%
Employee awareness and training programmes	26%
Multi-Factor Authentication	22%

KEY FINDINGS

The data reveals a near-identical perception of effectiveness across three key areas. Roughly a quarter identify endpoint detection, network segmentation and employee training as equally impactful. A slightly smaller proportion – just over a fifth – highlight Multi-Factor Authentication as most effective. This suggests a recognition of the importance of layered security, with a strong emphasis on both technical solutions and human awareness.

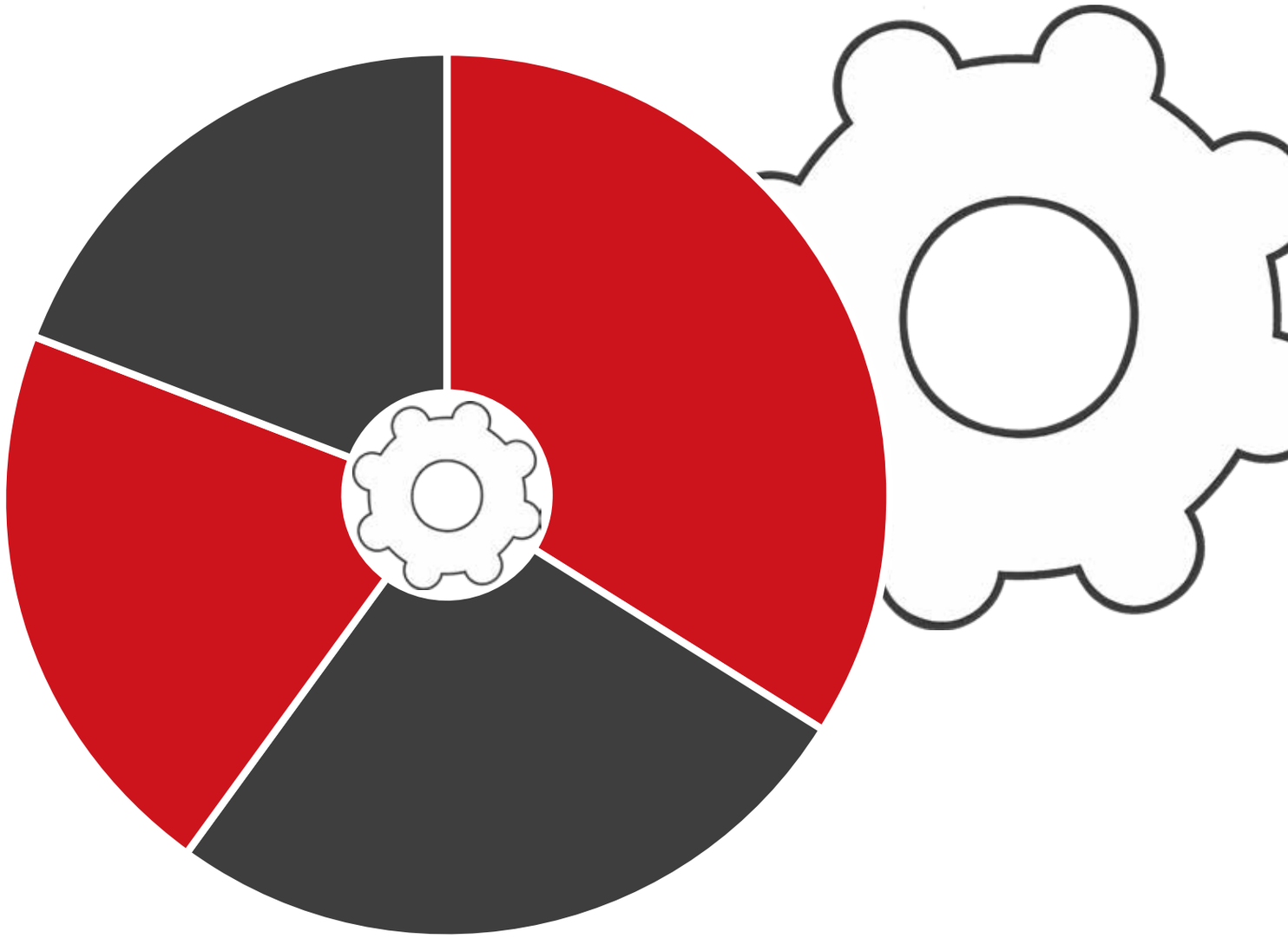
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 16

What factors are most influential on your organisation's cybersecurity investment decisions? Select two.



Emerging threat landscape	34%
Regulatory compliance requirements	26%
Risk of financial loss from breaches	21%
Client or stakeholder expectations	19%

KEY FINDINGS

Nearly a third of respondents cite the emerging threat landscape as the primary influence, with a further quarter highlighting regulatory compliance. A significant proportion, nearly half, acknowledge the risk of financial loss and client expectations. This indicates that investment decisions are predominantly driven by external pressures and the need to mitigate tangible risks.

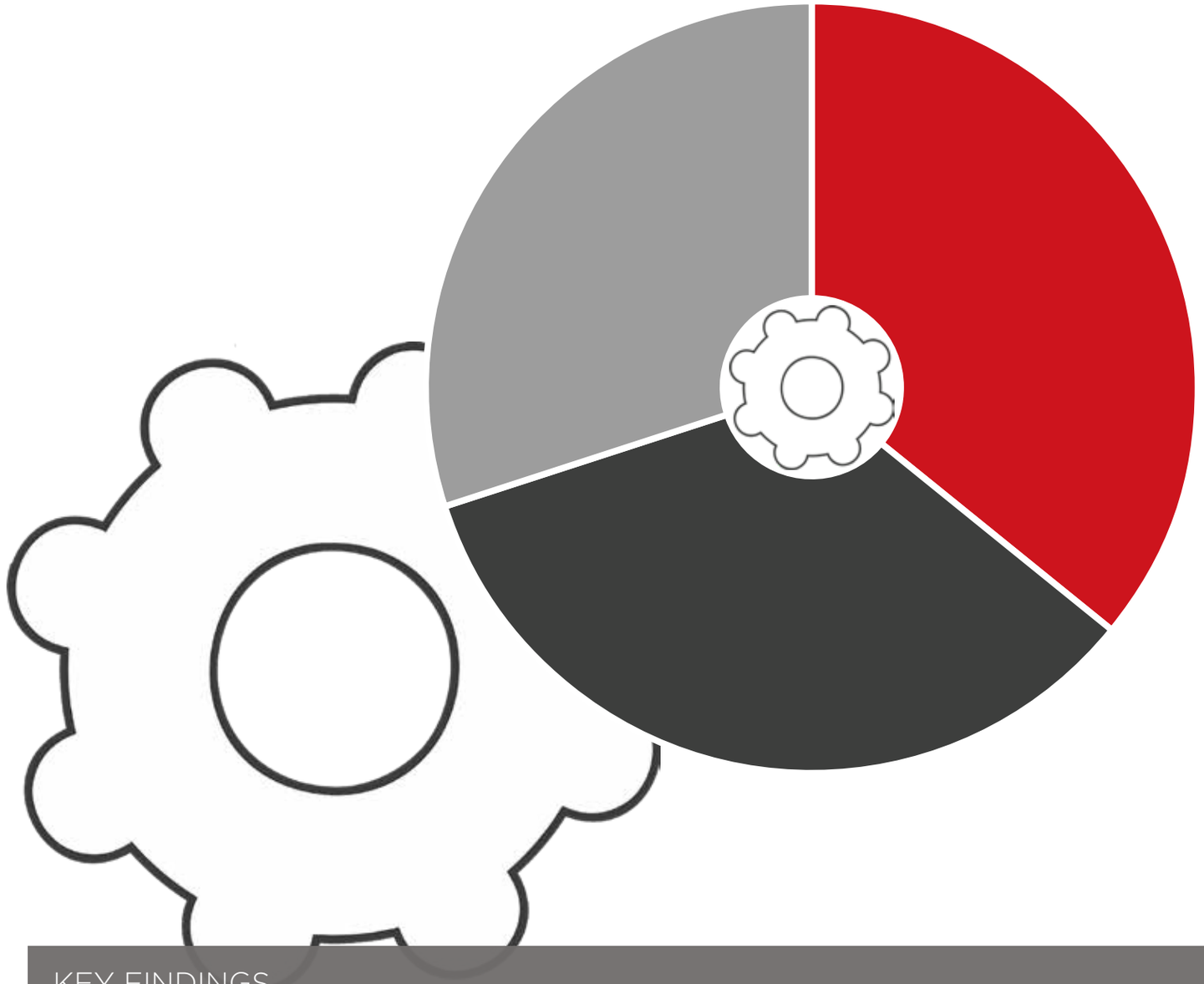
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 17

How satisfied are you with the cybersecurity tools and solutions currently in use within your organisation?



KEY FINDINGS

Roughly a third are ‘Unsatisfied’, with a similar proportion ‘Somewhat satisfied’ with their organisation’s current cybersecurity tools and solutions’. A slightly smaller, but still significant, proportion are ‘Very satisfied’. The fact that over a third of respondents (36%) are unsatisfied shows a critical need for tool evaluation and potential replacement, highlighting a potential vulnerability due to perceived inadequacies.

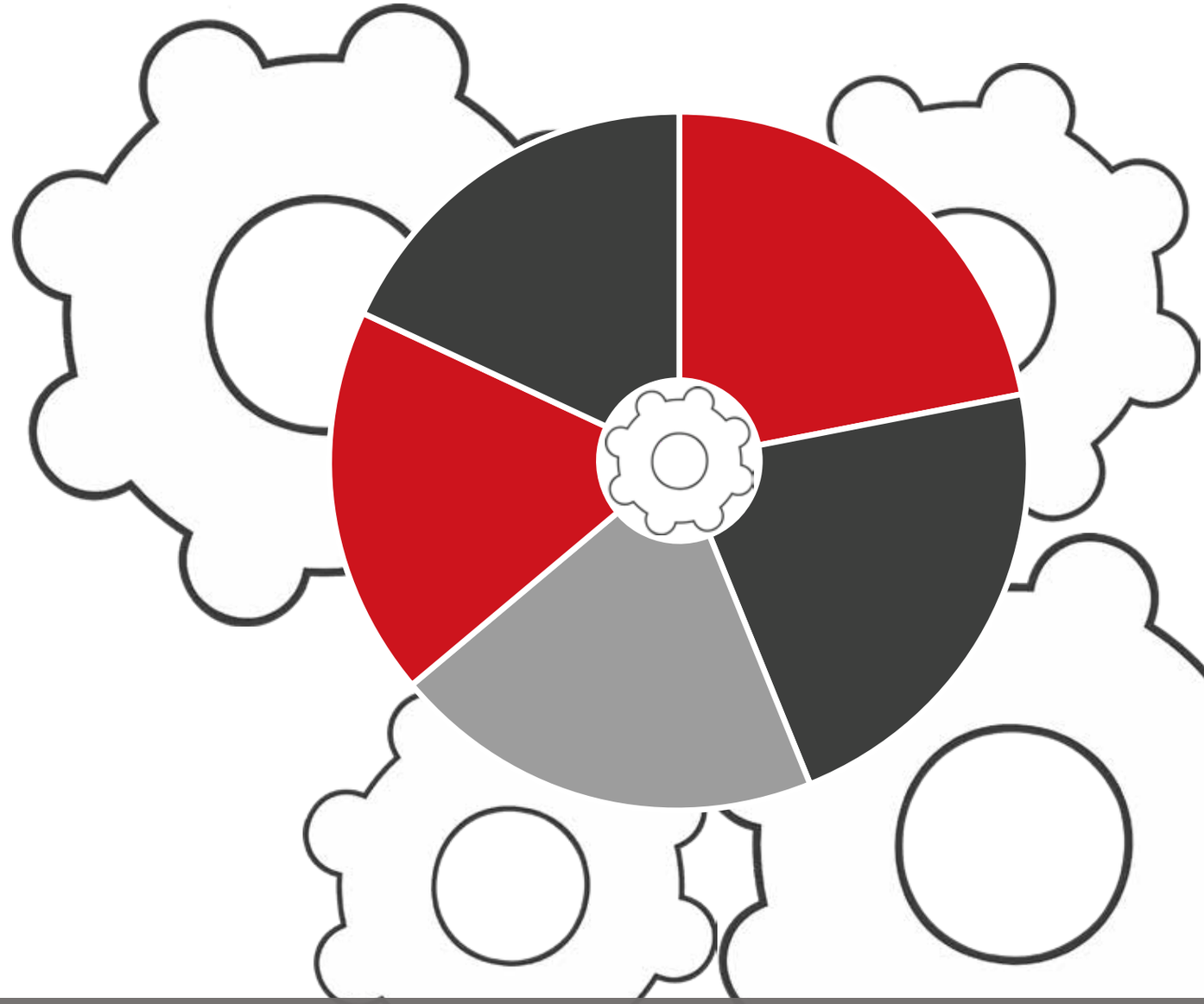
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 18

How does your organisation primarily consume threat intelligence? Select two.



Through automated feeds integrated into security tools	22%
Via structured intelligence reports and dashboards from commercial providers	22%
From information sharing communities and partnerships	20%
Our organisation doesn't consume threat intelligence	18%
Through analysis of industry sources and forums	18%

KEY FINDINGS

Equal fractions – each nearing a quarter – rely on automated feeds and commercial reports. A significant proportion also utilise community sharing. However, a concerning minority – almost a fifth – report no consumption. Overall, the data reveals a mix of passive and active intelligence gathering, with a notable gap in some organisations.

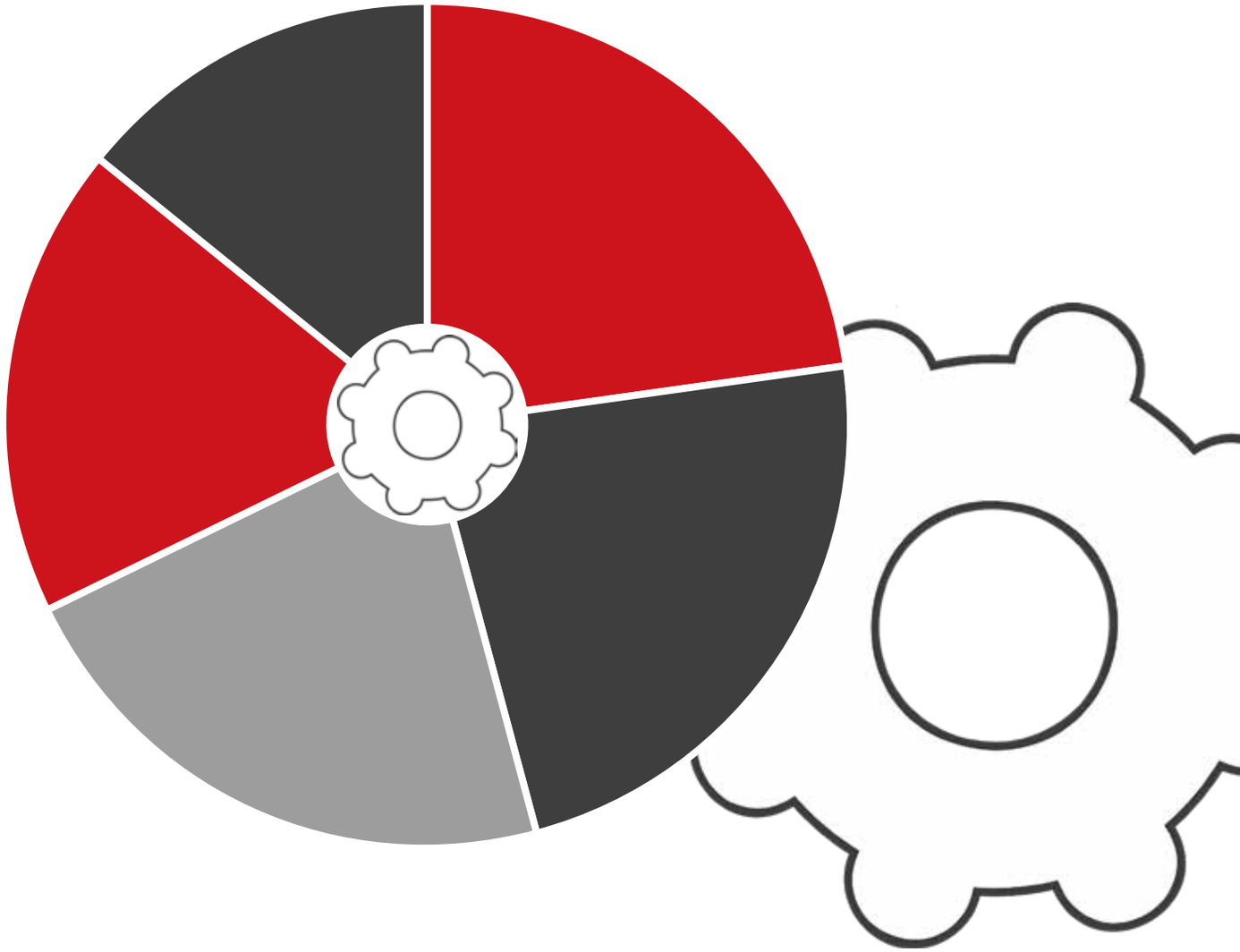
A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

QUESTION 19

What are the primary operational benefits you receive from threat intelligence? Select two.



Improved threat analysis	23%
Faster incident response	23%
Improved SOC efficiency	22%
Better prioritisation of security efforts	18%
We don't receive any noticeable benefit	14%

KEY FINDINGS

Roughly a quarter identify improved threat analysis and faster incident response as primary benefits. A significant proportion – almost half – also highlight improved SOC efficiency and better prioritisation. A notable fraction, nearly one-in-seven, perceive no benefit. This indicates a potential disconnect between threat intelligence implementation and realised operational gains, calling for a review of its effectiveness.

A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

CONCLUSION

"Endpoint security, advanced detection and Zero Trust architecture are set to dominate the strategic agenda in 2025, while emerging technologies like Quantum Computing begin to influence long-term planning."

As organisations continue to grapple with the complexity of the modern threat landscape, there is a prevailing sense of cautious optimism. Nearly a third of those surveyed rate their cybersecurity posture as 'excellent', with a further quarter indicating it is 'good' – a positive reflection of maturing capabilities. However, beneath this surface, significant challenges persist. Budget constraints remain the leading hurdle for nearly a quarter of respondents, followed closely by the difficulties posed by evolving threats and integration gaps.

Regulatory demands and the relentless pace of technological change further complicate the cybersecurity equation. Phishing attacks and weak password practices continue to be the most common and avoidable mistakes. Encouragingly, almost a third of organisations are prioritising preventative strategies and robust backups to mitigate ransomware risks.

Proactive threat intelligence and clear communication are increasingly recognised as key to individual and organisational resilience. The growing adoption of AI and Machine Learning – already leveraged by over half the organisations surveyed – demonstrates a collective shift towards enhancing threat detection and prevention capabilities. Endpoint security, advanced detection and Zero Trust architecture are set to dominate the strategic agenda in 2025, while emerging technologies like Quantum Computing begin to influence long-term planning.

Integration strategies remain fragmented, yet solutions like TIP, SOAR and IAM are gaining traction. Meanwhile, almost a quarter highlight the importance of network segmentation, endpoint detection and employee training in fortifying defences. Threat intelligence is consumed through a balance of automated feeds and commercial reports, with improved analysis and faster response being key benefits.

As attendees of this security focused event looking ahead, one thing is clear: organisations that will thrive in this dynamic environment are those that embrace a holistic approach – delivering unbiased, comprehensive, real-time and actionable threat intelligence to outpace adversaries and drive smarter, faster security decisions.

By

Krishan Parmar,
Senior Content Strategist,
Lynchpin Media

A Lynchpin Media BRAND

PRIORITIES
REPORTS, EVENTS & WEBINARS

Recorded Future®

CLICK TO EXPERIENCE SOME OF OUR OTHER REPORTS

Lynchpin Media

Lynchpin Media is a global technology media, data and marketing services company. We help to increase awareness, develop and target key accounts and capture vital information on regional trends.

Find out more:
lynchpinmedia.com

PRIORITIES
REPORTS, EVENTS & WEBINARS

CxO Priorities, a Lynchpin Media Brand
63/66 Hatton Garden
London, EC1N 8LE
United Kingdom

Find out more:
www.cxopriorities.com

Recorded Future®

Find out more:
www.recordedfuture.com