A Lynchpin Media BRAND

priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات
GISEC GLOBAL

MIDDLE EAST SECURITY TRENDS AND PRIORITIES REPORT 2024

A priorities Report

in collaboration with

معرض و مؤتمر الخليج العالمي لأمن المعلومات
GISEC GLOBAL

In conjunction with intelligent CISO security intelligence that transcends borders and INTELLIGENT CIO Providing Unparalleled Technology Intelligence MIDDLE EAST

A Lynchpin Media BRAND

cxo priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

CONTENTS

A Lynchpin Media BRAND

CXO priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

INTRODUCTION

SURVEY OVERVIEW

To find out more about the current cybersecurity and IT challenges facing enterprises in the Middle East, we surveyed 150 CISOs and those in similar roles to find out about the key challenges they're encountering, how they anticipate AI will impact the industry and how they're planning for future investment. The report aims to present an overview of the current cyberthreat landscape, explore the complexities of managing cybersecurity and reveal how organisations plan to prioritise and invest.

We are living in a truly digital age where technology is revolutionising every daily activity we complete. Whether it's accessing healthcare services, managing finances through online banking, engaging in remote education, shopping via e-commerce platforms, or optimising manufacturing processes through automation and data analytics, technology is omnipresent.

As technology continues to advance at an unprecedented rate, its impact on various sectors will only deepen, reshaping the way we live, work and interact with the world around us.

However, this digitalisation means the attack surface has expanded rapidly, with malicious actors presented with a plethora of opportunities to target organisations. Against a backdrop of an increasingly complex and sophisticated threat landscape and business challenges such as a cyberskills shortage and awareness training, Chief Information Security Officers (CISOs) face multiple challenges as they strive to secure their organisations' digital assets.

The emergence of AI is also providing opportunities to attackers and the rising simplicity with which attacks can be executed is a concern among industry professionals. However, AI also holds immense potential as a game-changer for defenders, providing advanced capabilities to strengthen cyberdefences and mitigate emerging threats.

CISOs in the Middle East certainly agree that AI will be a force for good to the industry according to our research, with 83% supporting this sentiment – a testament to the widespread optimism regarding the potential of the technology.

This CXO Priorities research sheds light on the key challenges faced by CISOs in their daily roles and identifies the investment priorities that will shape the future of cybersecurity.

A Lynchpin Media BRAND

priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات
GISEC GLOBAL

CHAPTER 1
THE THREAT LANDSCAPE AND ORGANISATIONAL CYBER POSTURE

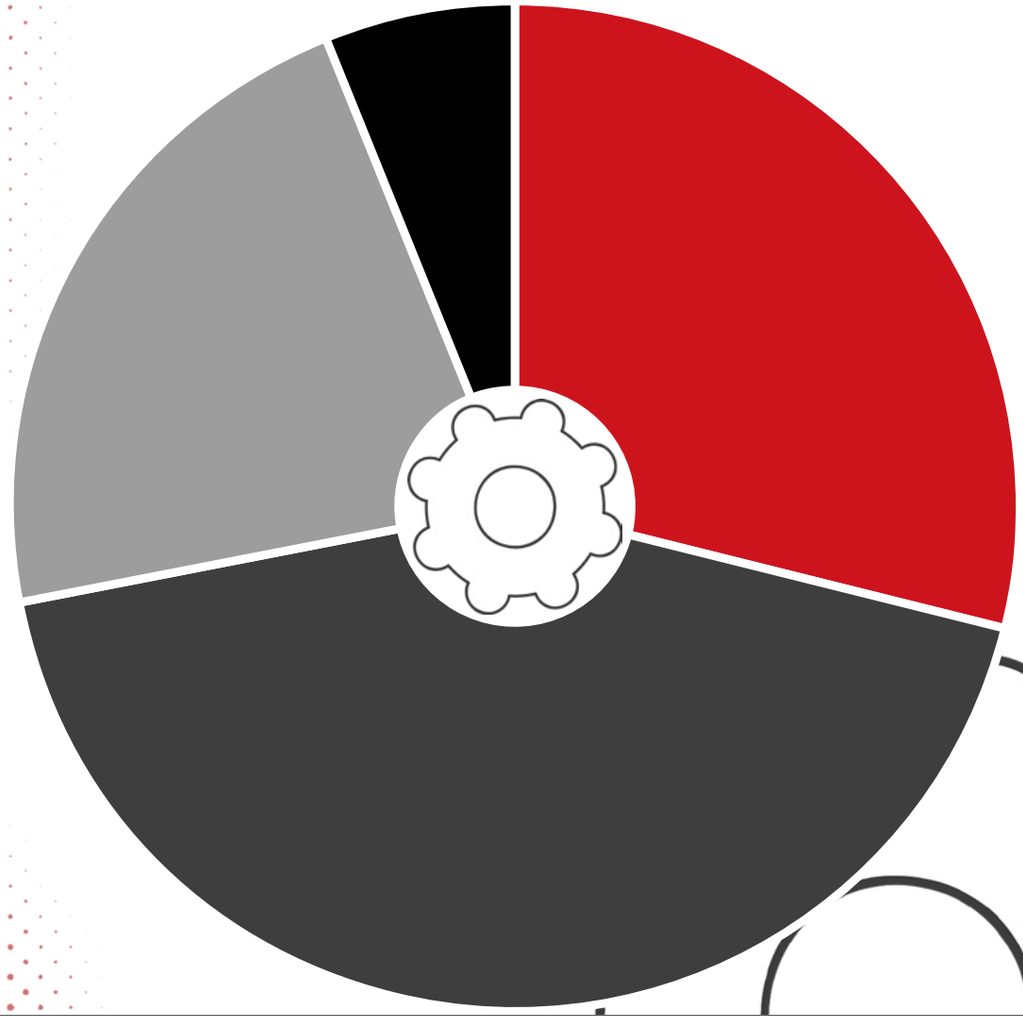
A Lynchpin Media BRAND

CXO priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

QUESTION 1

How confident are you in your organisation's ability to defend against emerging cyberthreats?



- Very confident 29%
- Confident 43%
- Satisfied 22%
- Not very confident 6%

KEY FINDINGS

More than two-thirds of respondents cite a level of confidence (43% 'confident' and 29% 'very confident') while 22% are 'satisfied' in their organisation's ability to defend against emerging threats, indicating a generally positive outlook. However, 6% of CISOs stated they were not confident showing there are improvement areas for cybersecurity readiness. Organisations must exercise continual vigilance and focus on investment in cybersecurity measures to effectively tackle emerging threats.

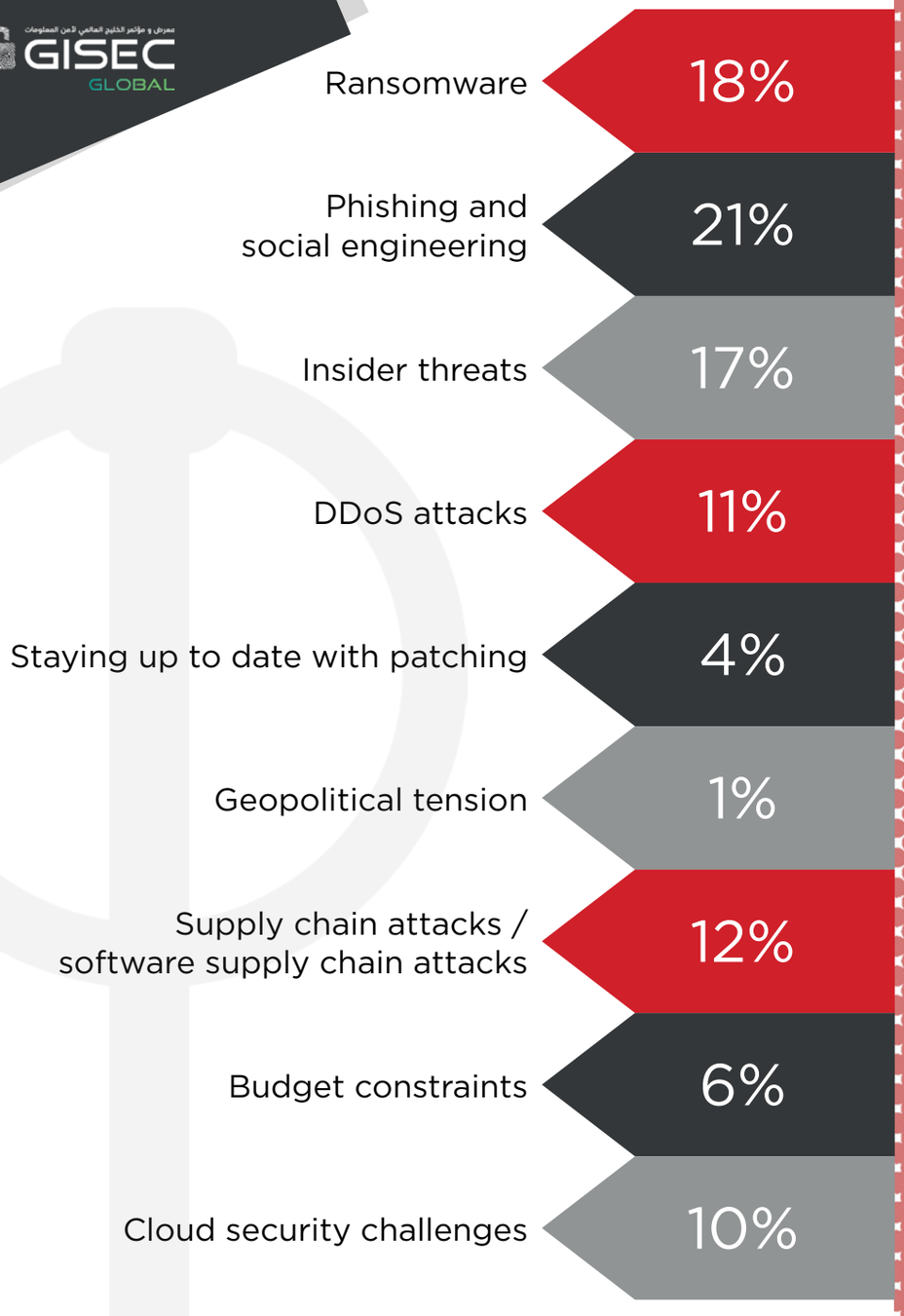
A Lynchpin Media BRAND

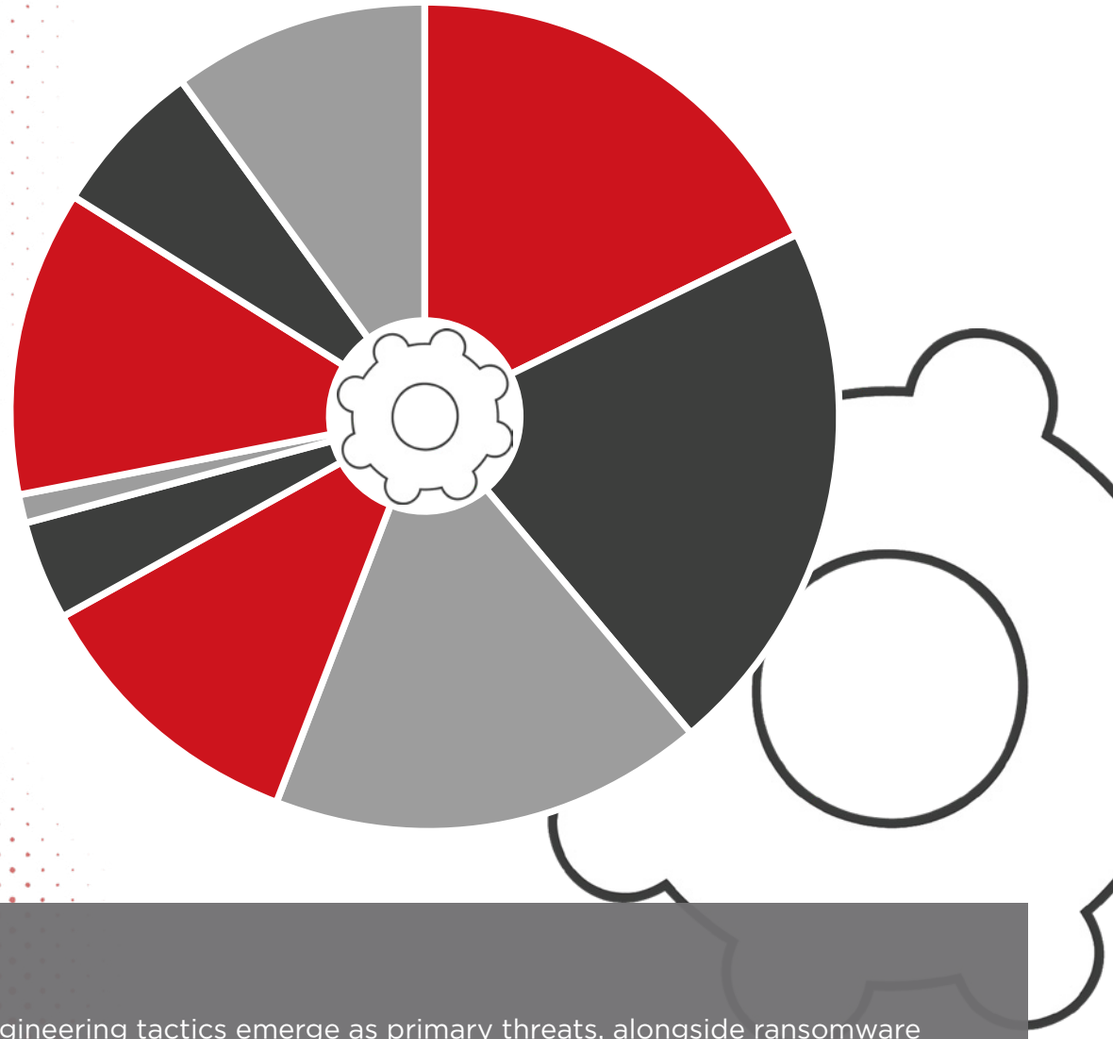
cxo priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

QUESTION 2

In the past 12 months, what have been the top two most significant cybersecurity challenges faced by your organisation?





KEY FINDINGS

Phishing and social engineering tactics emerge as primary threats, alongside ransomware incidents, reflecting the persistent risk posed by deceptive tactics and extortion malware. Insider threats and supply chain vulnerabilities also warrant attention, highlighting the significance of internal risks and inter-organisational dependencies. Addressing these multifaceted challenges demands a holistic approach encompassing robust defence mechanisms, employee awareness training and strategic risk mitigation strategies.

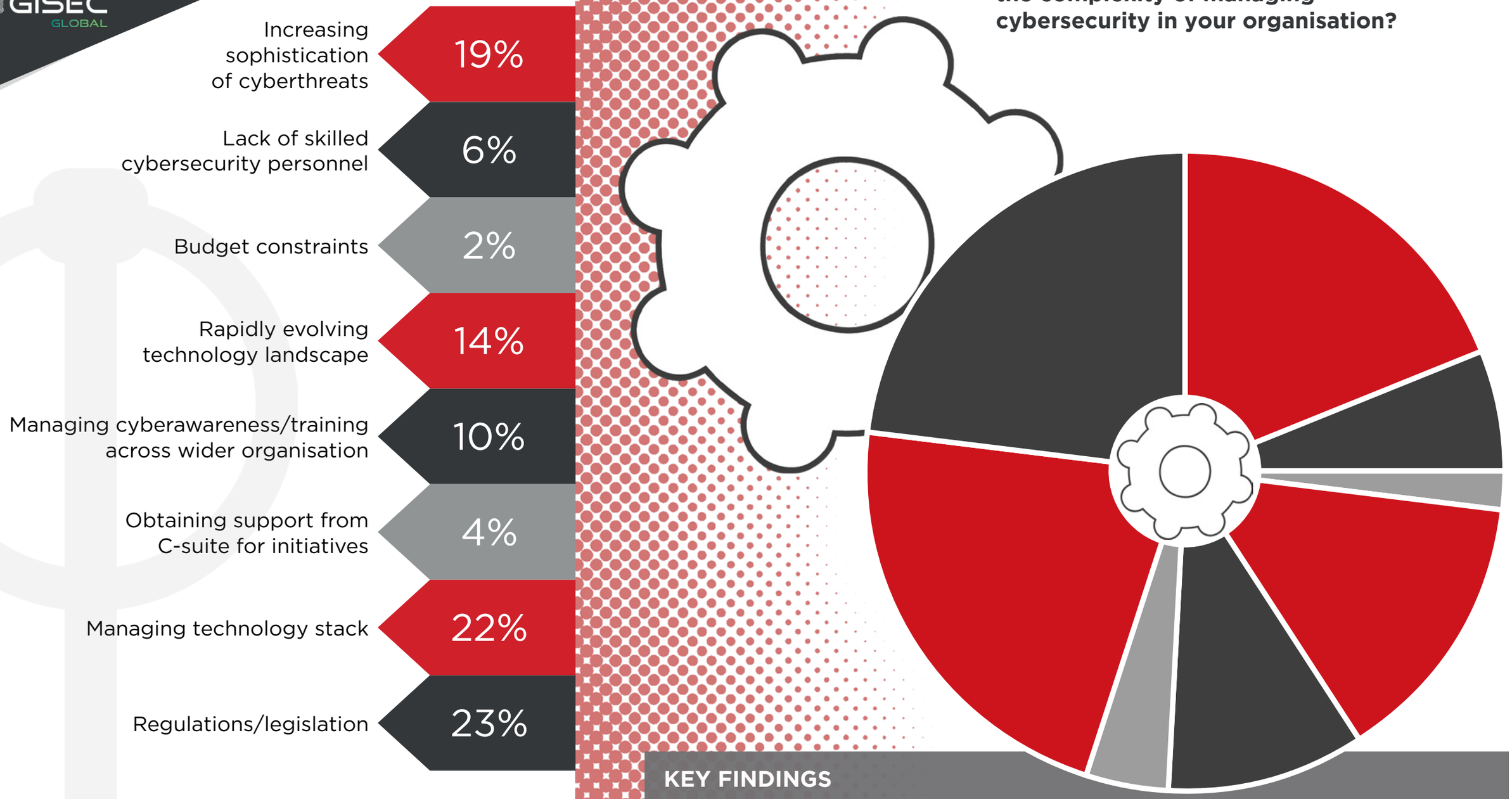
A Lynchpin Media BRAND

CXO priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

QUESTION 3

What factors contribute most to the complexity of managing cybersecurity in your organisation?



KEY FINDINGS

Regulations and legislation are the top factors which contribute most to the complexity of managing cybersecurity, followed closely by managing the technology stack, pointing toward the complexities of integrating and maintaining diverse security technologies. The rapidly evolving technology landscape exacerbates this challenge, requiring continual adaptation.

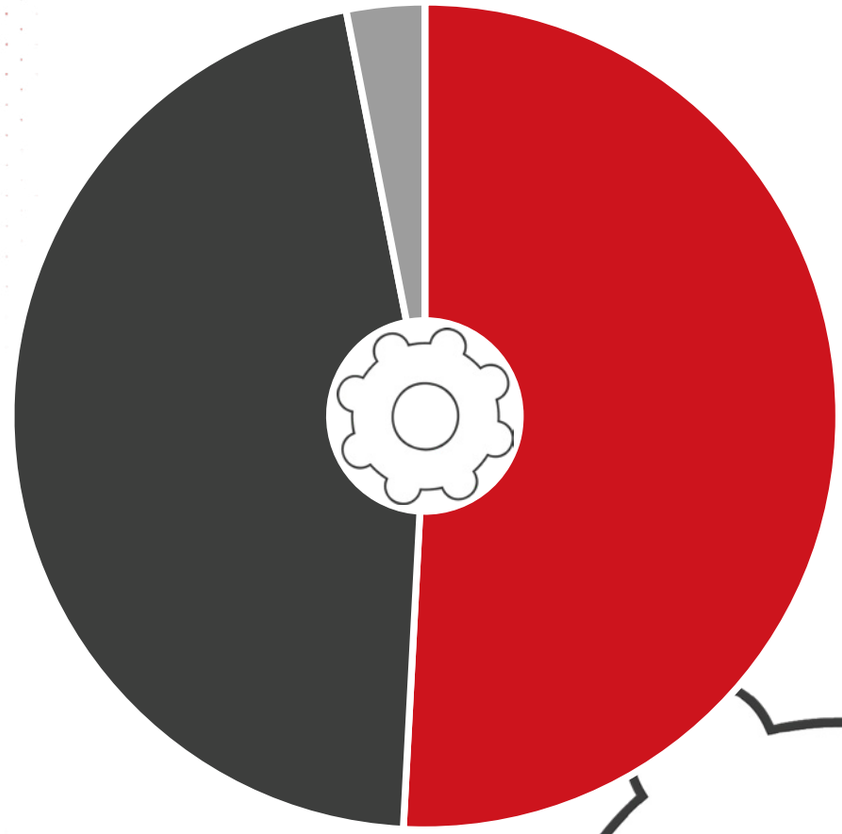
A Lynchpin Media BRAND

cxo priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

QUESTION 4

How confident are you that employees within your organisation can effectively recognise and report cybersecurity threats?



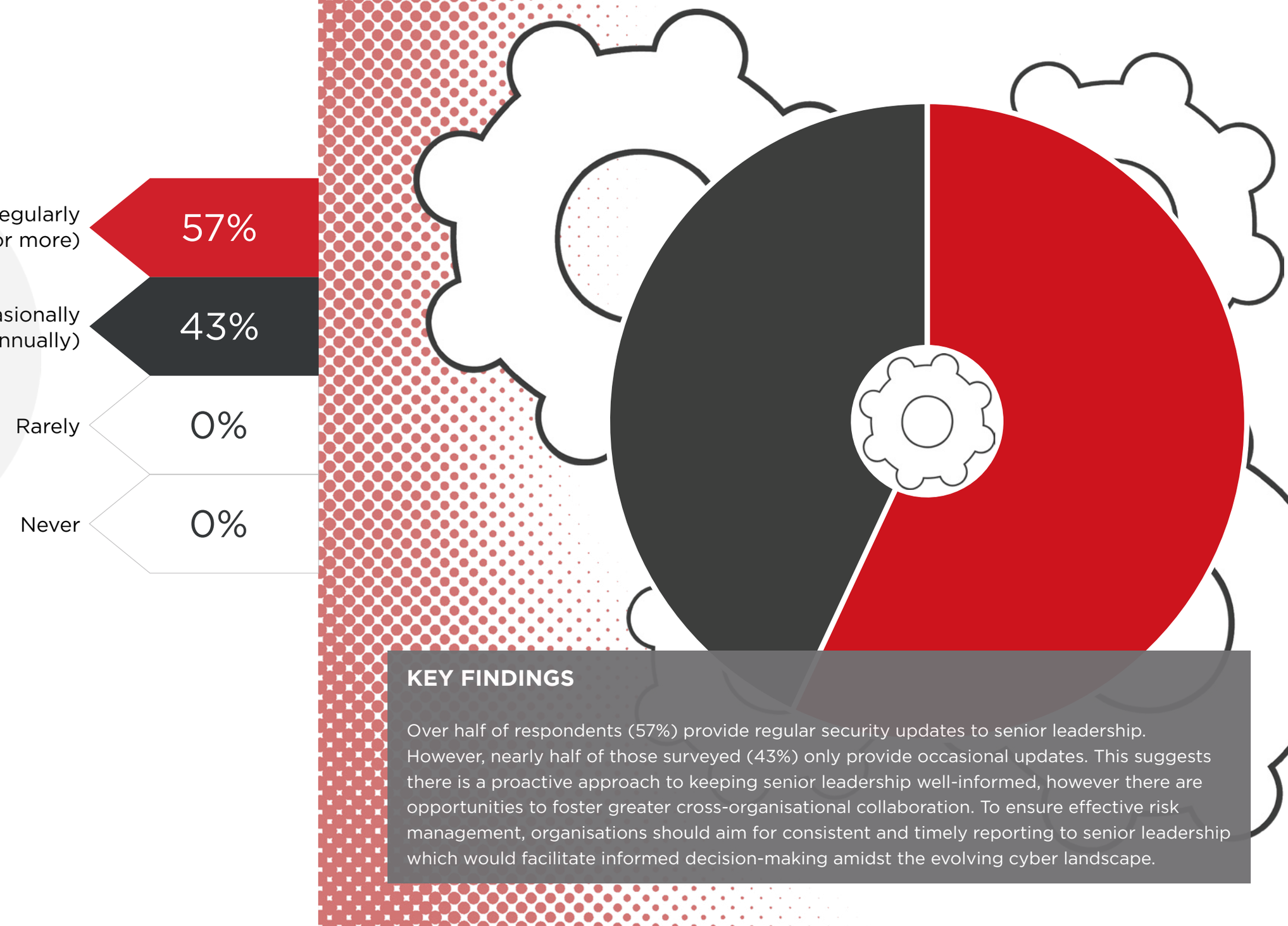
Very confident	51%
Confident	46%
Satisfied	3%
Not confident	0%

KEY FINDINGS

Nearly all respondents (97%) said they were either confident (46%) or very confident (51%) in their employees' abilities to recognise and report threats. This indicates confidence in cyberawareness and training strategies. It is recommended that companies continue investing in ongoing reinforcement and upskilling to ensure employees remain vigilant against evolving cyberthreats.

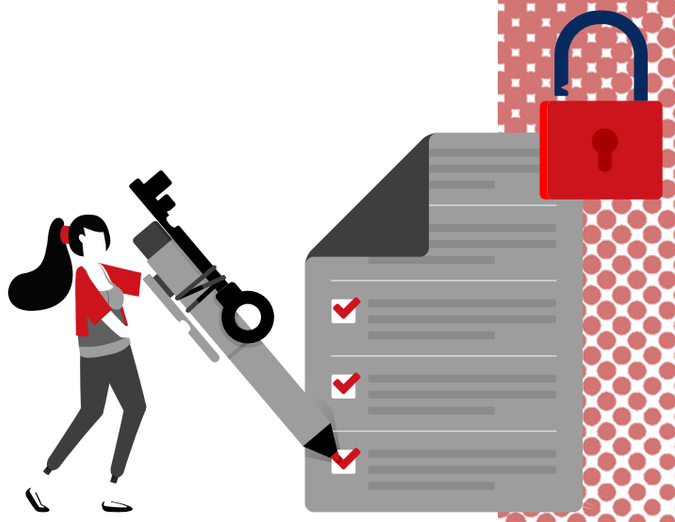
QUESTION 5

How frequently do you provide updates or reports on the organisation's cybersecurity posture to senior leadership?



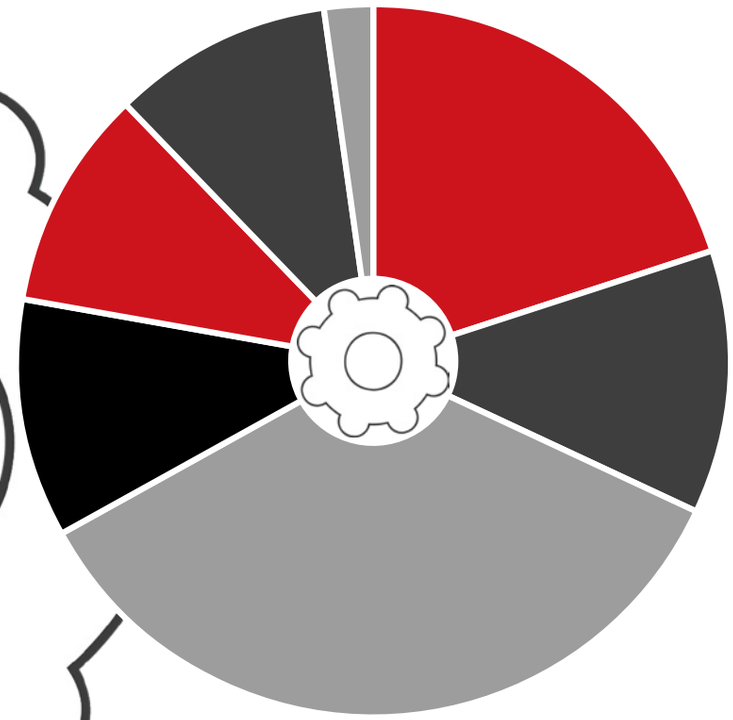
KEY FINDINGS

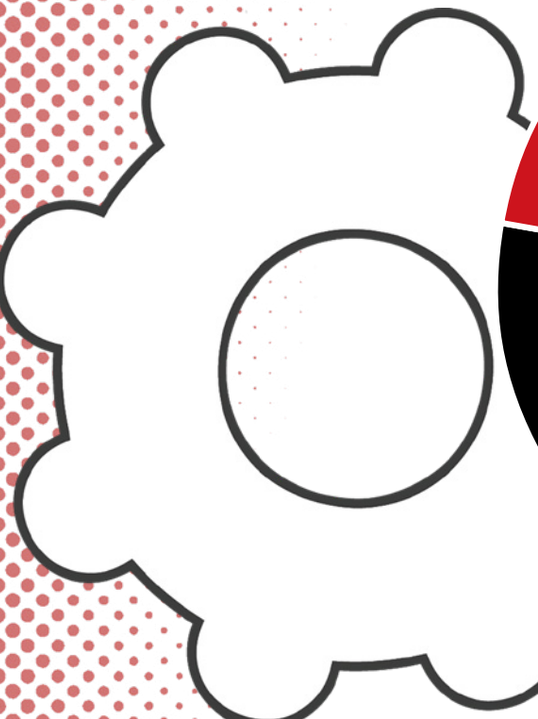
Over half of respondents (57%) provide regular security updates to senior leadership. However, nearly half of those surveyed (43%) only provide occasional updates. This suggests there is a proactive approach to keeping senior leadership well-informed, however there are opportunities to foster greater cross-organisational collaboration. To ensure effective risk management, organisations should aim for consistent and timely reporting to senior leadership which would facilitate informed decision-making amidst the evolving cyber landscape.

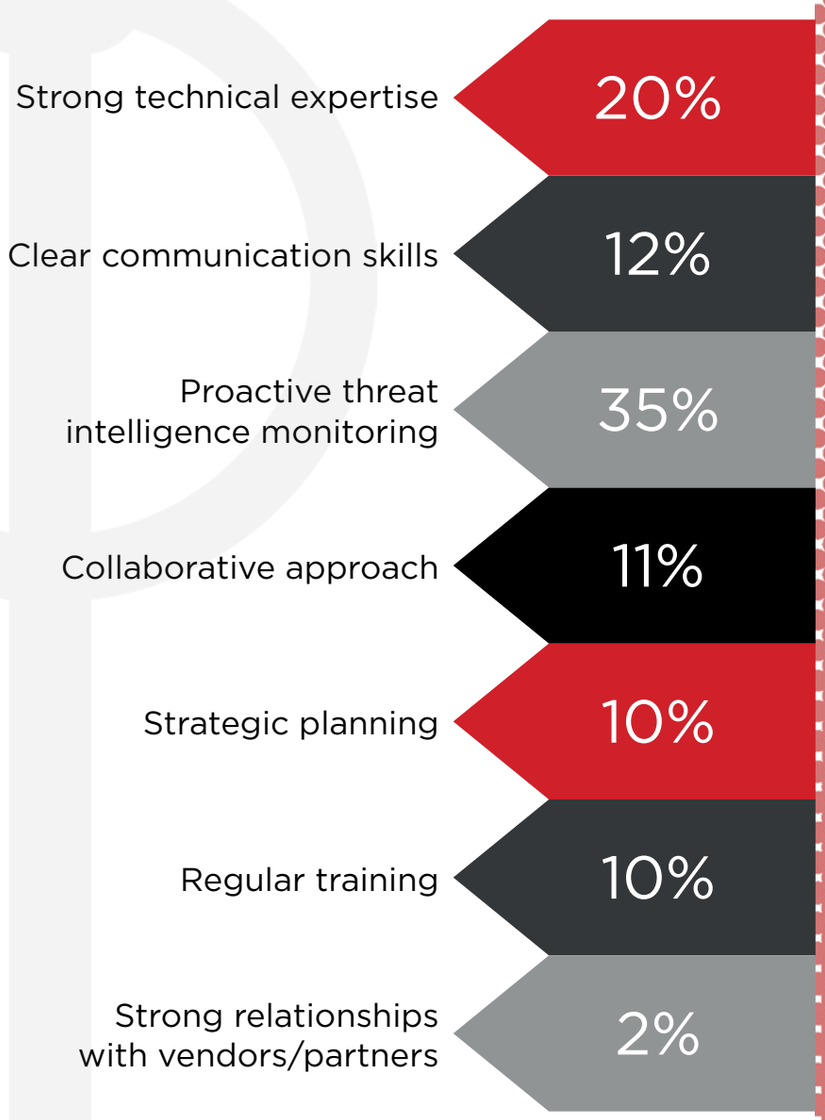


QUESTION 6

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







KEY FINDINGS

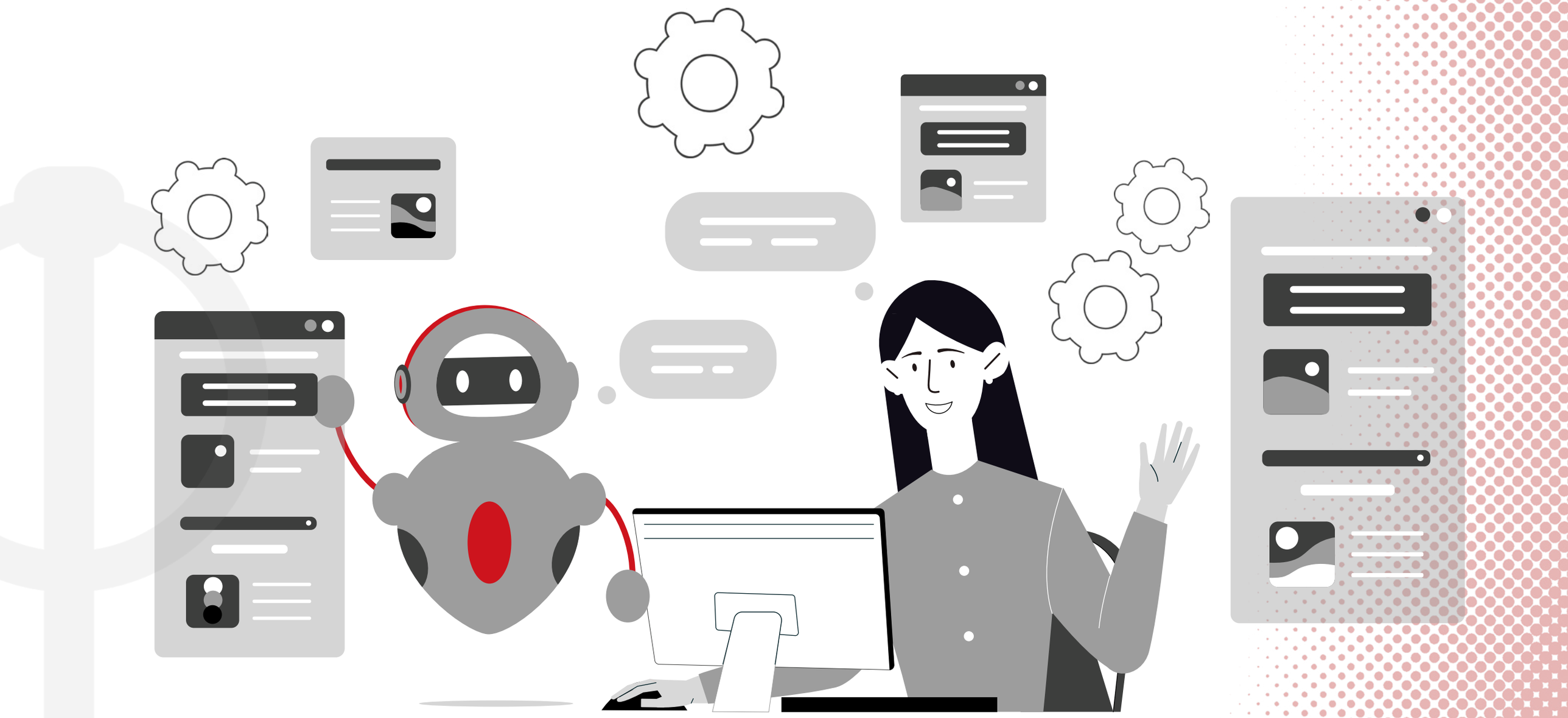
More than one-third of respondents cite proactive threat intelligence monitoring (35%) as the most important factor when manging cybersecurity threats. A total of 20% also state that strong technical expertise plays a vital role in navigating complex threats. Furthermore, clear communication skills (12%) facilitate effective dissemination of security information. A collaborative approach (11%) fosters cross-functional synergy, while strategic planning (10%) ensures alignment with organisational objectives. Regular training (10%) underscores the importance of continual learning. However, the low emphasis on relationships with vendors/partners (2%) suggests potential for leveraging external expertise. These insights highlight the diverse skill set required for effective cybersecurity management.

A Lynchpin Media BRAND

CXO priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

CHAPTER 2
AI IN CYBERSECURITY



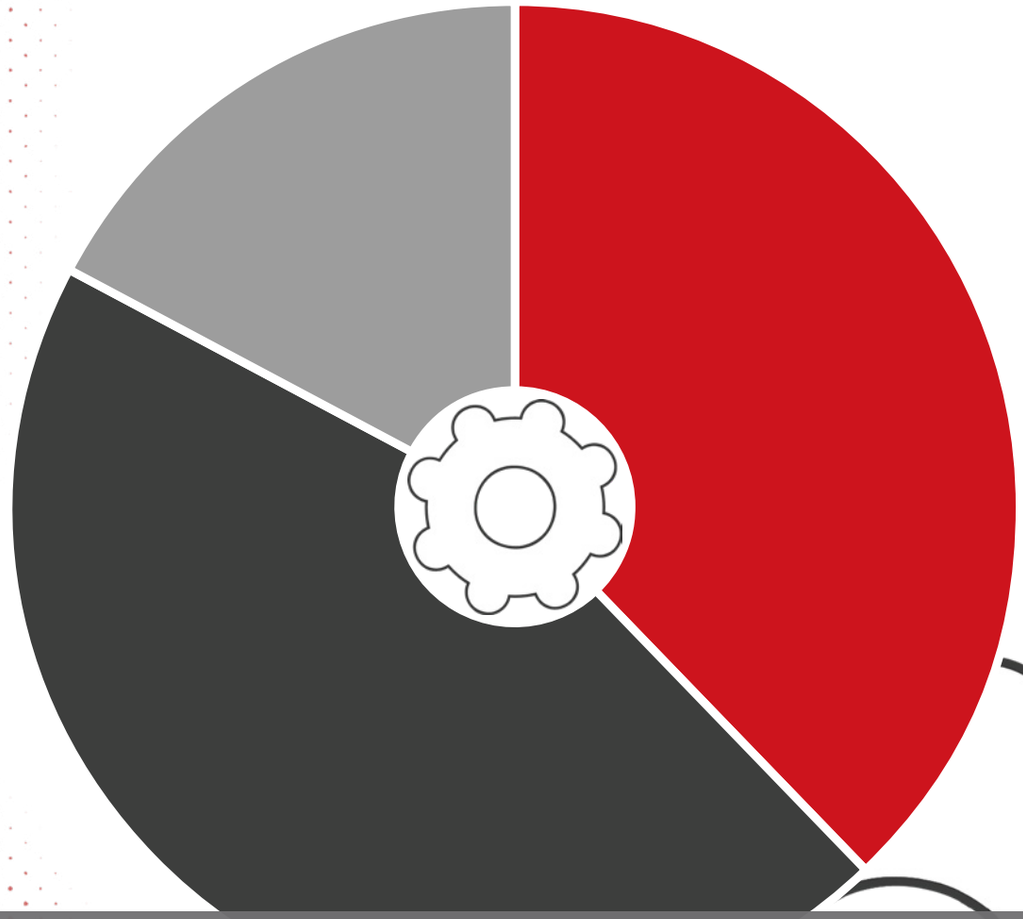
A Lynchpin Media BRAND

cxo priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

QUESTION 7

How far do you agree with the following statement: 'AI will be a force for good for cybersecurity'?



Strongly agree	38%
Agree	45%
Disagree	17%
Strongly disagree	0%

KEY FINDINGS

An overwhelming majority of CISOs in the Middle East believe AI will be a force for good for their industry. While AI is still in the early stages of development and attackers are leveraging the technology for their own gains, it is reassuring to hear that the industry generally concedes that it will be beneficial in levelling the playing field.

More than 80% of those surveyed either strongly agreed (38%) or agreed (45%) with this sentiment. This should serve as a nod to the opportunity AI presents to the industry.

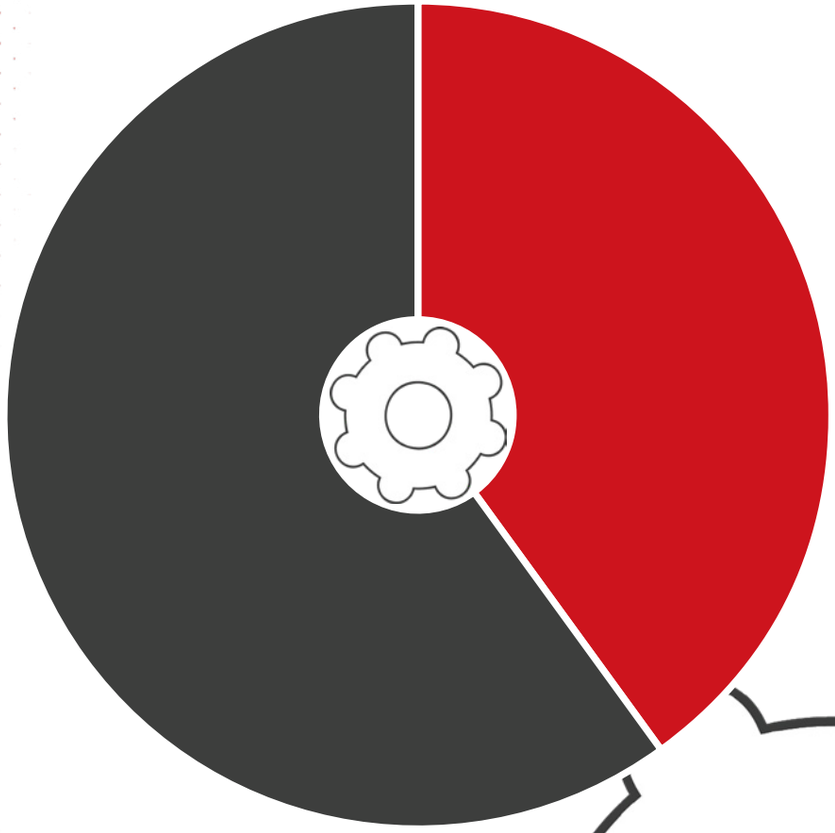
A Lynchpin Media BRAND

cxo priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

QUESTION 8

How would you describe your organisation's readiness to deploy Artificial Intelligence (AI) solutions for cybersecurity?



Fully prepared	40%
Preparing to deploy	60%
No plans for AI deployment	0%
I don't know	0%

KEY FINDINGS

All respondents said their organisation was looking to deploy AI solutions for cybersecurity, with 40% stating they were 'fully prepared' and 60% indicating they were 'preparing to deploy'. This highlights the direction that the industry is taking when it comes to integrating AI into security strategies. As the technology continues to evolve, CISOs will look to AI solutions to support their overall aims.

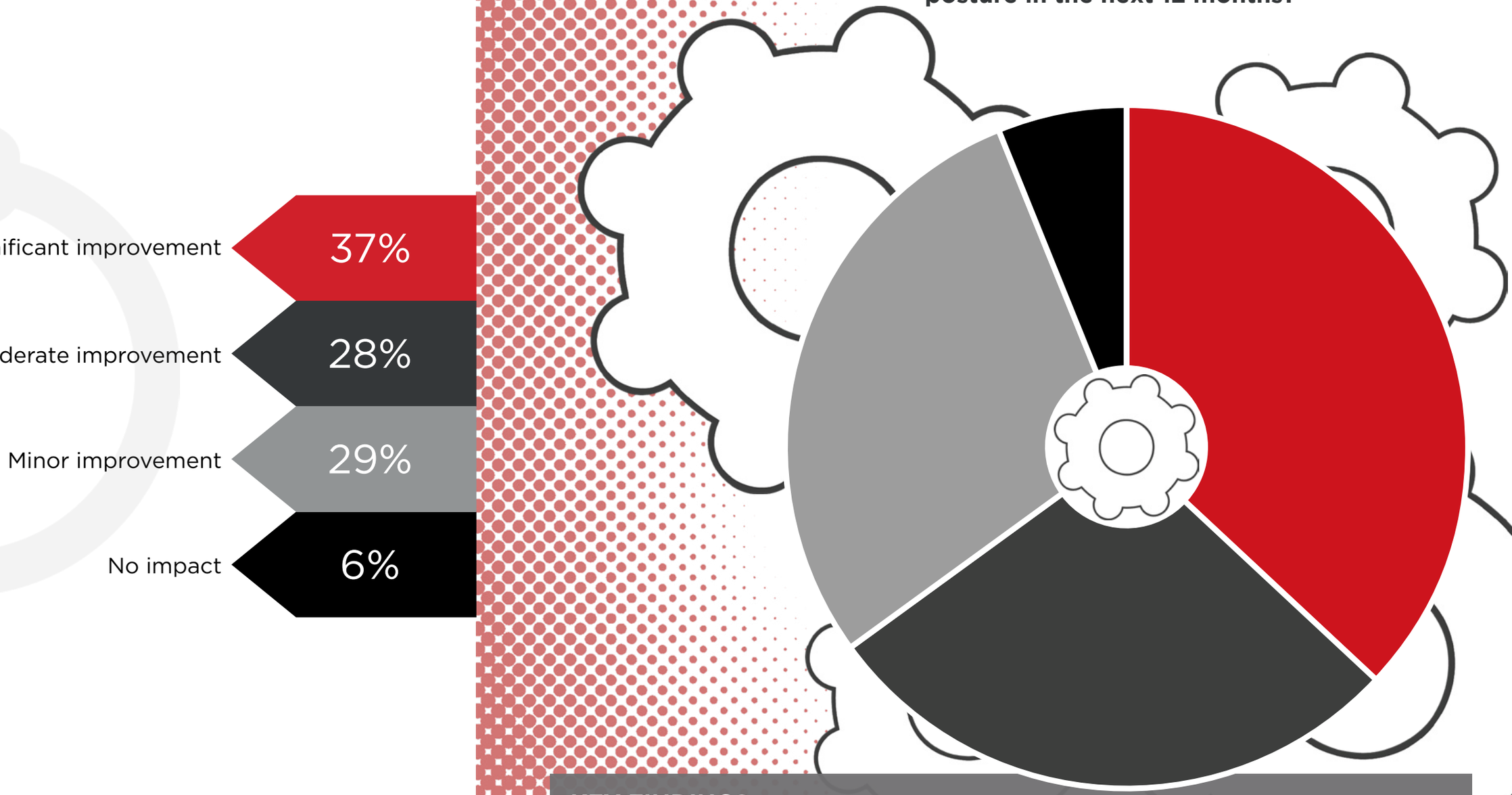
A Lynchpin Media BRAND

cxo priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

QUESTION 9

What role do you foresee AI playing in enhancing your organisation's cybersecurity posture in the next 12 months?



KEY FINDINGS

A majority of respondents foresee AI enhancing their organisation's cybersecurity posture within the next year – with 37% anticipating a significant improvement, 28% a moderate improvement and 29% a minor improvement within the next year.

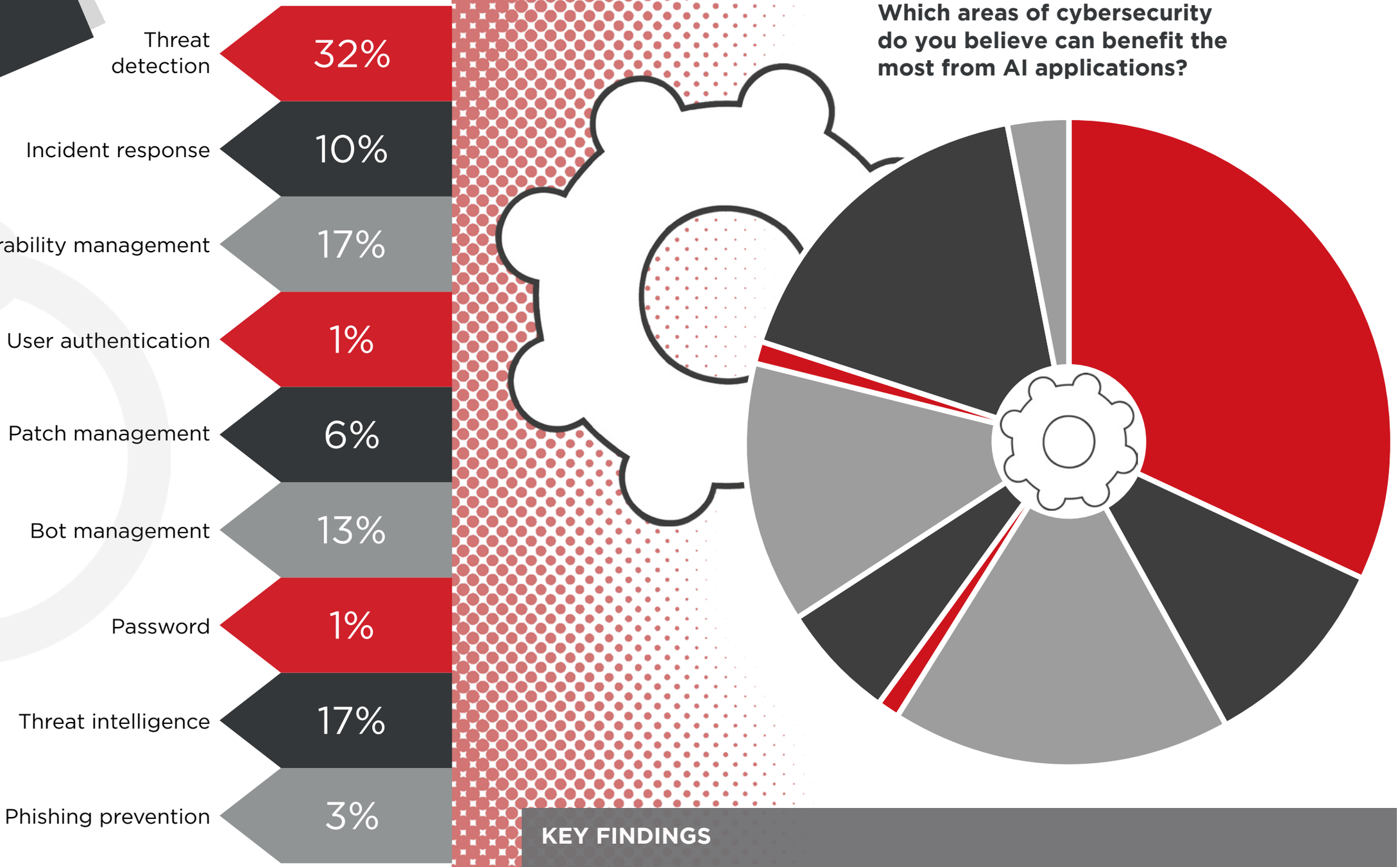
A Lynchpin Media BRAND

cxo priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

QUESTION 10

Which areas of cybersecurity do you believe can benefit the most from AI applications?



KEY FINDINGS

Cybersecurity professionals expect threat detection, vulnerability management and threat intelligence to be key areas which will benefit most from AI. With AI able to process vast amounts of data quickly, as well as analyse patterns and anomalies in data, there are opportunities for cybsersecurity teams to get ahead of attackers.

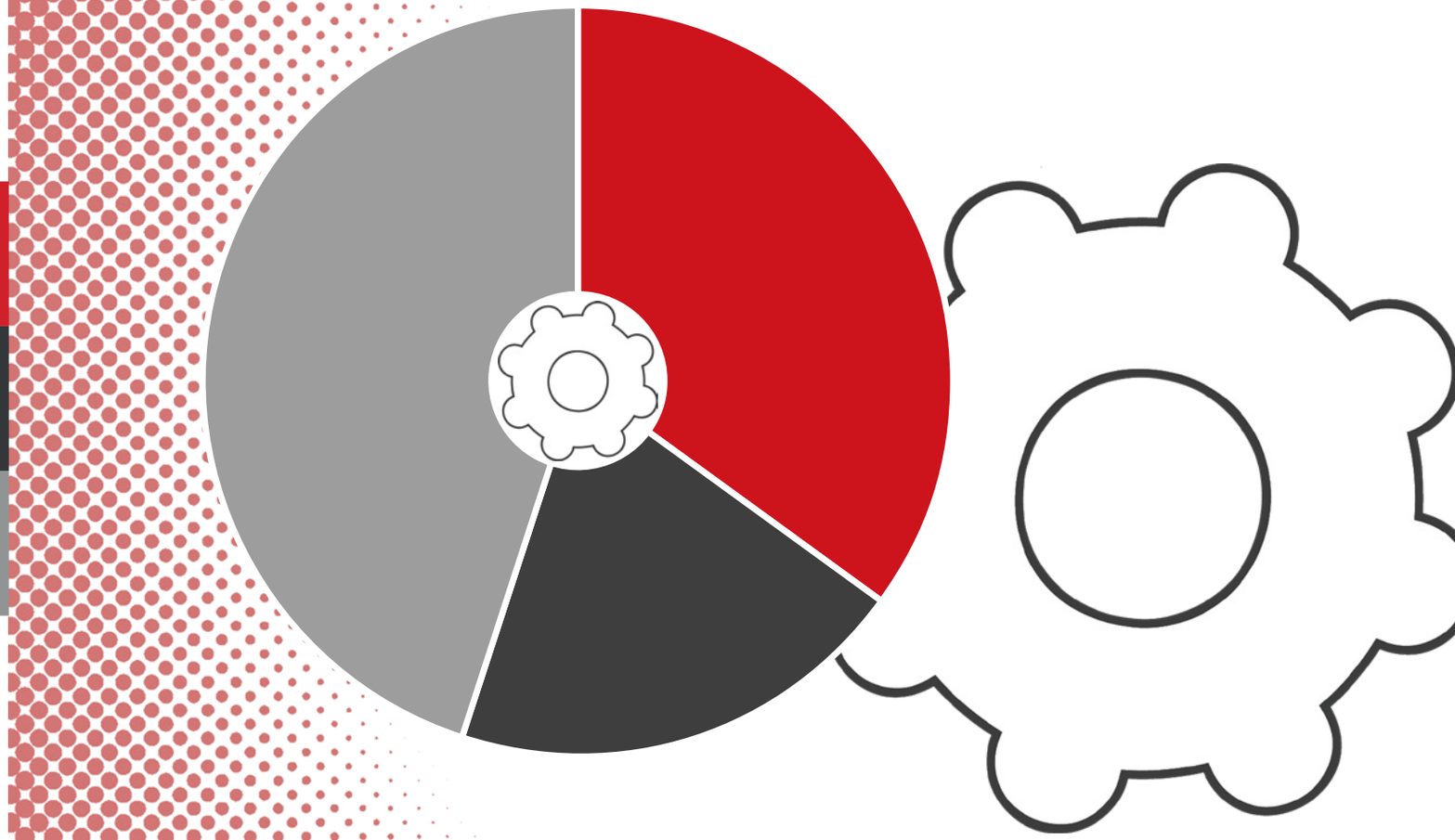
A Lynchpin Media BRAND

CXO priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

QUESTION 11

In your view, how will AI impact cybersecurity?



It will even the playing field between attackers and defenders — 35%

It will enable attackers to gain the upper hand — 20%

It will enable defenders to gain the upper hand — 45%

KEY FINDINGS

As highlighted throughout this report, AI has become a major talking point across the global IT playing field. Organisations far and wide are adapting their business models to make way for AI's capabilities, particularly when it comes to cybersecurity. Our data shows 35% of people we spoke to believe it will even the playing field between attackers, while 20% think it will enable attackers to gain the upper hand. A large percentage of people we surveyed (45%) believe AI will enable defenders to gain the upper hand – an interesting result.

A Lynchpin Media BRAND

CXO priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

CHAPTER 3
PRIORITIES FOR CYBER LOOKING AHEAD

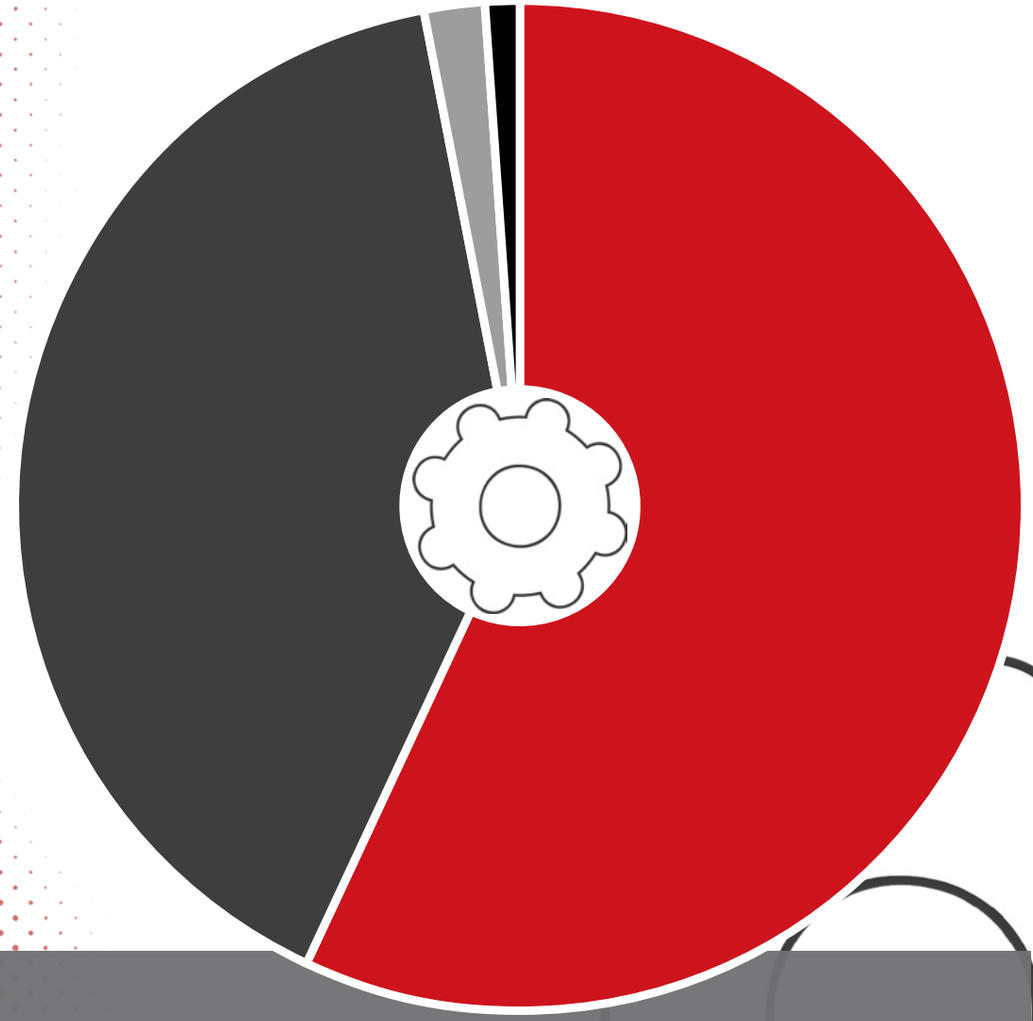
A Lynchpin Media BRAND

cxo priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

QUESTION 12

Compared to 2023, how has your budget for cybersecurity changed for 2024?



The budget has increased by more than 10%	57%
The budget has increased by less than 10%	40%
There has been no change – the budget has remained the same	2%
The budget has decreased by more than 10%	1%

KEY FINDINGS

On the change in cybersecurity budgets for 2024, 57% reported a substantial increase of more than 10% while 40% indicated a moderate increase of less than 10%. A minimal 2% reported no change signifying a consistent budget and only 1% noted a decrease exceeding 10%. This suggests a prevailing positive shift in budget allocations to highlight the increasing need for cybersecurity within organisations, signalling a growing recognition of its importance in today's rapidly evolving threat landscape.

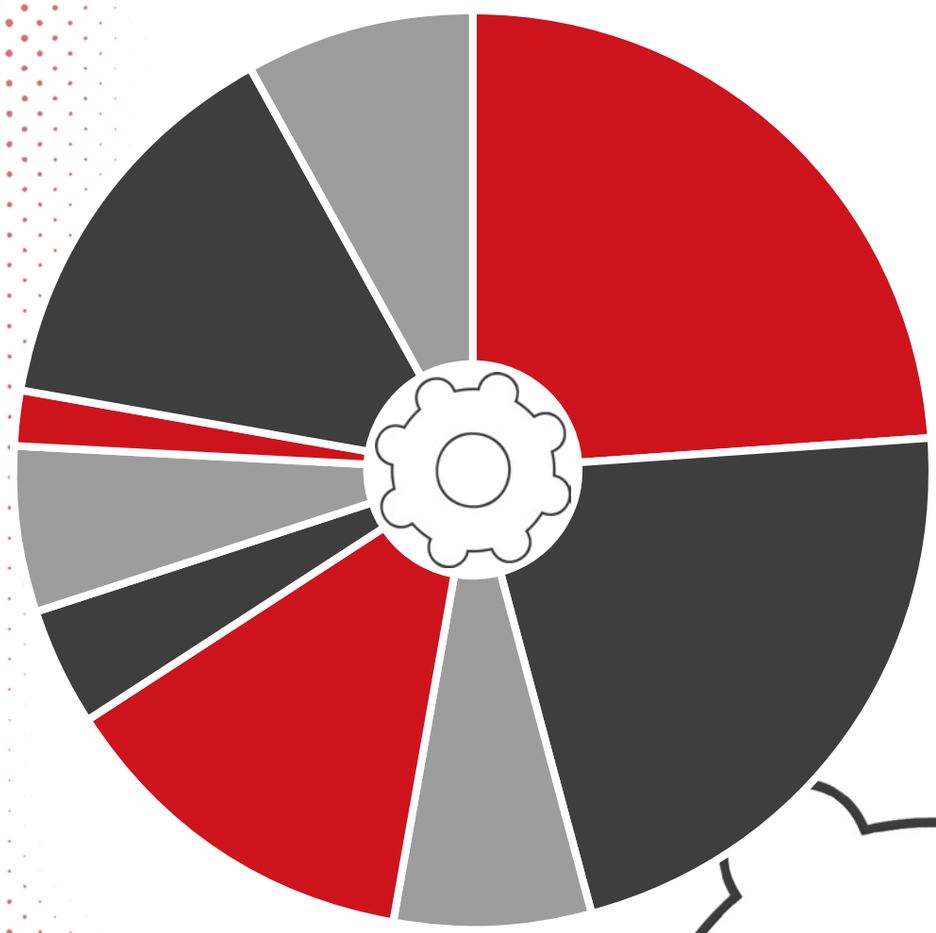
A Lynchpin Media BRAND

CXO priorities

GISEC GLOBAL

QUESTION 13

What are your top two investment areas over the next 12 months?



- Advanced threat detection: 24%
- Cloud security: 22%
- Endpoint security: 7%
- Identity and access management: 13%
- Network security: 4%
- Awareness and training: 6%
- Email security: 2%
- Incident response: 14%
- Exploring AI tools: 8%

KEY FINDINGS

Advanced threat detection and cloud security are the top two investment areas for organisations in the next 12 months. This is closely followed by incident response highlighting a commitment to swift and effective action in the face of potential threats. Identity and access management emerge as a key concern for 13% of respondents. This investment trend reflects a strategic alignment with the evolving cybersecurity challenges organisations face, demonstrating a proactive stance in fortifying their digital infrastructure against advanced threats and ensuring robust cloud security measures.

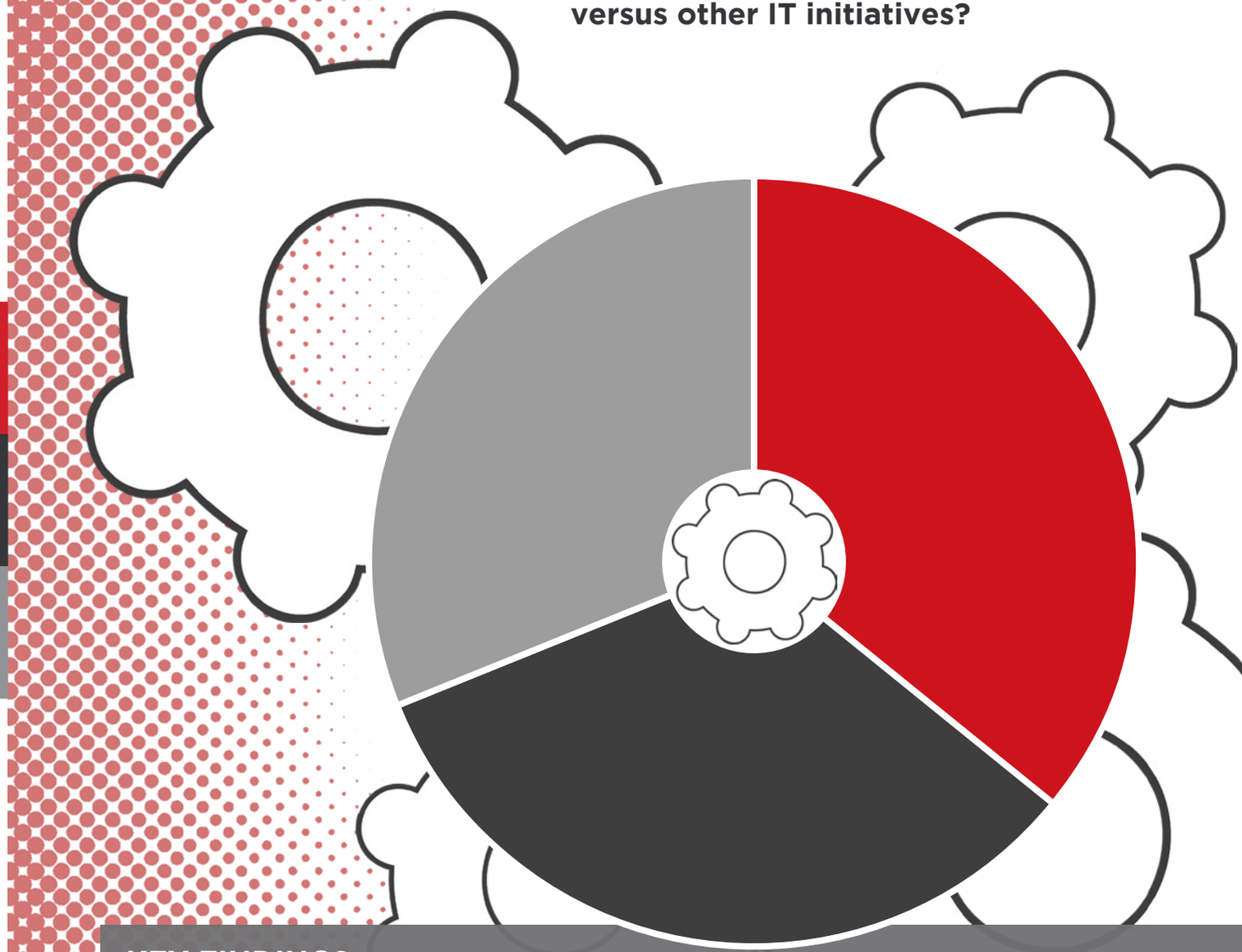
A Lynchpin Media BRAND

cxo priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات
GISEC GLOBAL

QUESTION 14

How does your organisation prioritise investments in cybersecurity versus other IT initiatives?



High priority	36%
Medium priority	33%
Low priority	31%

KEY FINDINGS

In evaluating organisational investment priorities between cybersecurity and other IT initiatives, 36% identified cybersecurity as a high priority, closely followed by 33% allocating a medium priority. Notably, 31% considered cybersecurity a low priority within their investment spectrum. This data indicates the varied emphasis placed on cybersecurity across organisations and highlights the need for tailored strategies to address the distinct priorities and risk perceptions in the cybersecurity landscape.

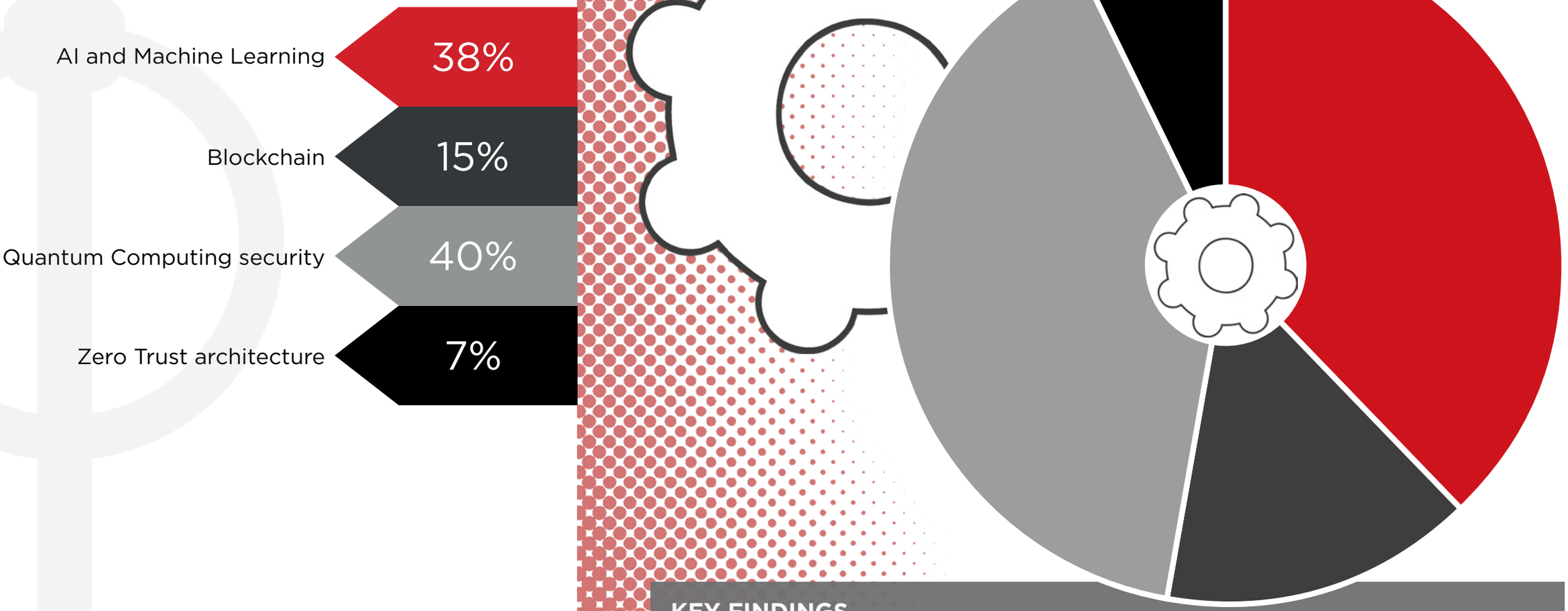
A Lynchpin Media BRAND

CXO priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات GISEC GLOBAL

QUESTION 15

In terms of cybersecurity, what emerging technologies do you consider crucial for future investments?



KEY FINDINGS

Participants highlighted Quantum Computing security and Artificial Intelligence (AI) and Machine Learning (38%) as their most crucial priorities for future investments. This is closely followed by Blockchain at 15% and Zero Trust architecture at 7%. The key takeaway from the data underscores a compelling emphasis on Quantum Computing security, reflecting a growing recognition of its critical role in shaping the future landscape of cybersecurity investment.

CONCLUSION

The cybersecurity landscape is complex, not only due to the diverse range of threats that proliferate, but also the business challenges that CISOs are grappling with daily.

Cybersecurity is a concern for every organisation, with all verticals united by a core challenge – keeping the bad guys out.

While the survey findings highlight a generally positive outlook among cybersecurity professionals regarding their organisation's ability to defend against emerging threats, there is more to be done to cast this confidence even wider, emphasising the need for continual vigilance and investment in cybersecurity measures.

With phishing and social engineering and insider threats positioned within the top three cybersecurity challenges identified by CISOs, there is a need for tailored cyberawareness and training to keep the 'human' line of defence robust. Ransomware also remains a key threat so technology investments should ensure this is considered.

Addressing the complexities in managing cybersecurity – including regulations, managing the technology stack and the rapidly evolving technology landscape – demands comprehensive strategies encompassing technology, personnel and regulatory compliance.

The widespread belief in AI as a force for good in the cybersecurity industry reflects optimism about its potential to level the playing field against attackers. Organisations are actively looking to deploy AI solutions for cybersecurity, with the majority indicating preparedness or active preparation for deployment which hints at the future direction of the industry.

Investment trends reveal a positive shift in cybersecurity budgets, with a substantial increase reported by the majority of respondents. Advanced threat detection and cloud security are identified as top investment areas, highlighting a strategic alignment with evolving cybersecurity challenges.

Looking ahead, participants prioritise investments in Quantum Computing security and AI/ML, reflecting a recognition of their critical role in shaping the future landscape of cybersecurity.

In conclusion, the findings emphasise the importance of leveraging AI for cybersecurity to navigate the threat landscape effectively. Organisations must remain proactive, adaptable and committed to fostering a culture of cyber-resilience to safeguard against emerging threats in an increasingly digital world.

By

Jess Abell,
Director, Strategic Content,
Lynchpin Media

A Lynchpin Media BRAND

priorities

معرض و مؤتمر الخليج العالمي لأمن المعلومات
GISEC GLOBAL

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.

Visit lynchpinmedia.com for more information.

priorities

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

Find out more:
www.cxopriorities.com

معرض و مؤتمر الخليج العالمي لأمن المعلومات
GISEC GLOBAL

Dubai World Trade Centre

Find out more:
www.gisec.ae