Trellix

The Mind of the CISO:

Closing the gap between reaction and readiness

Insights from global CISOs on strategically operationalizing threat intelligence to build resilience, accelerate response, and stay ahead of evolving threats.

Contents page

Introduction

The role of the Chief Information Security Officer (CISO) has never been more critical or more complex. What was once a primarily technical position is now a strategic leadership role, with CISOs expected to manage risk and resilience, board-level communication, cross-functional alignment, and long-term planning in an environment of relentless change.

Against this backdrop, the threat landscape continues to evolve at pace. From the rise of AI-powered attacks to the growing coordination between threat actors, CISOs face mounting pressure to stay ahead of adversaries who are faster, more resourced, and more organized than ever. Yet while the threats are accelerating, so are the tools, technologies, and opportunities available to those tasked with defense.

At the heart of this evolving cybersecurity equation is threat intelligence. When applied strategically, threat intelligence can empower CISOs to make faster, better-informed decisions, anticipate risk before it materializes, and build resilience into the core of their operations. However, the reality for many is still far from this ideal. Threat intelligence often remains siloed, underused, or reactive, and disconnected from broader strategic planning.

This edition of Mind of the CISO seeks to understand what's holding organizations back from unlocking the full value of threat intelligence, and what the most forward-thinking leaders are doing to move from awareness to advantage. Based on in-depth research with 500 global CISOs, the report explores:

- The evolving threat landscape – including ransomware, nation-state attacks, and the rise of AI-powered attacks
- The need for and the challenge of adopting operational threat intelligence
- The role of AI and automation in combating threats
- The value of peer communities in navigating complexity and driving strategic clarity

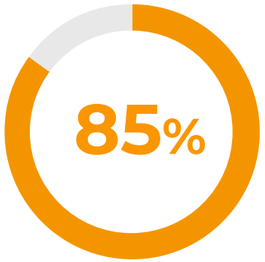
What becomes clear is technology alone isn't the answer. AI and automation will play a powerful role in enablement efforts, enhancing detection, reducing manual burden, and accelerating response, but cannot replace the strategic judgement of human leaders. Neither can CISOs succeed in isolation.

Trusted communities are emerging as critical spaces for shared insight, peer validation, and decision support.

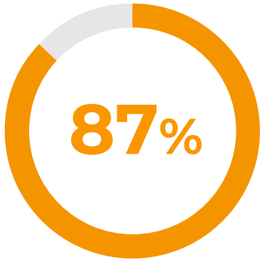
As the threat landscape becomes more collaborative, so must the defenders. Threat intelligence isn't just about knowing more; it's about doing more with what you know. And the CISOs best equipped for the future will be those who embed threat intelligence into the very foundation of their leadership.

Key Findings

The evolving threat landscape – including ransomware, nation-state attacks, and the rise of AI-powered attacks



of CISOs agree their organization's cybersecurity budget is influenced by the volume of nation-state threats



of CISOs agree their organization's cybersecurity strategy is influenced by geopolitical tensions, such as nation-state threats

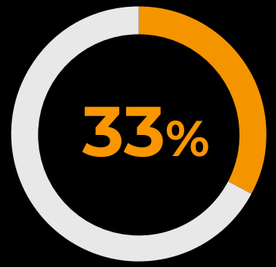
The need for and the challenge of adopting operational threat intelligence

of CISOs report their organization faces barriers when acting on threat intelligence

of organizations have not fully integrated threat intelligence into their wider cybersecurity strategy

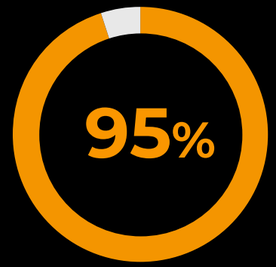
of organizations report they are taking a proactive approach to using threat intelligence for cybersecurity purposes

The role of AI and automation in combating threats

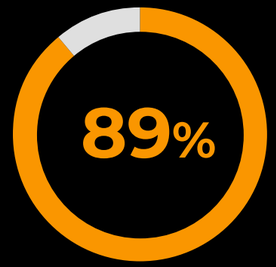


of CISOs believe AI-driven analytics would best help them perform their responsibilities more effectively

The value of peer communities in navigating complexity and driving strategic clarity



of CISOs agree being part of a threat intelligence sharing community or network improves their ability to prepare for threats

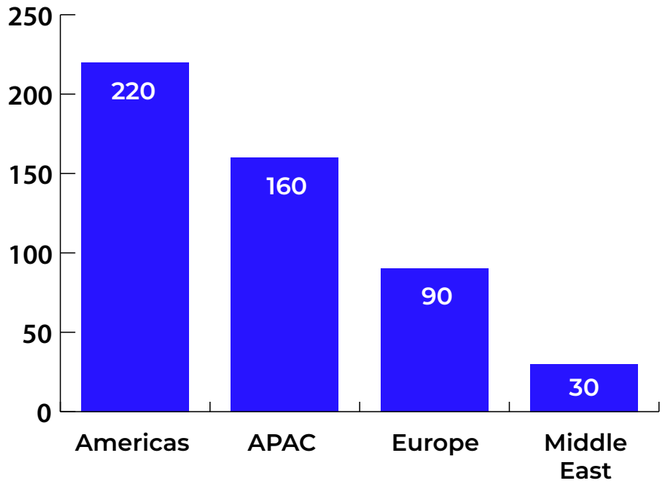


agree a CISO community would enable security leaders to navigate high-stakes decisions through trusted insights and shared experiences

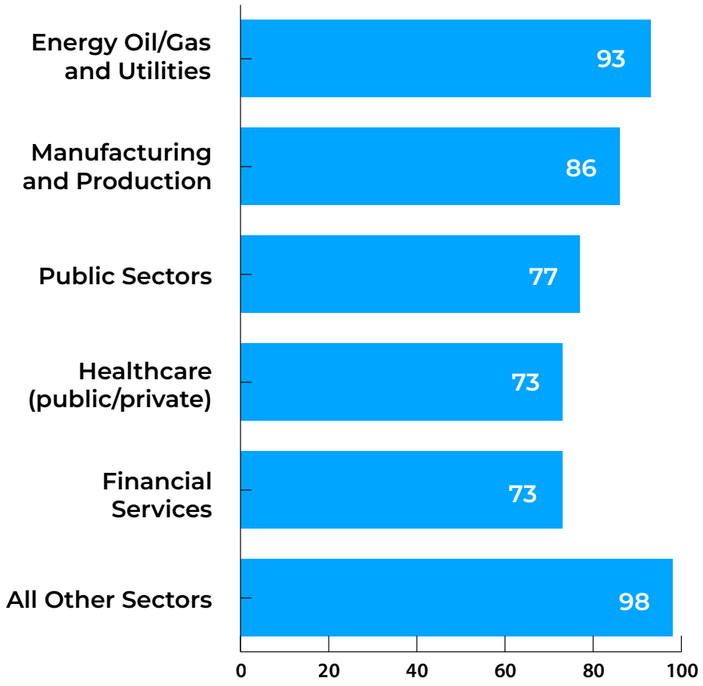
Quantitative respondents

500 CISOs (or equivalent) were interviewed in March/April 2025, split in the following ways:

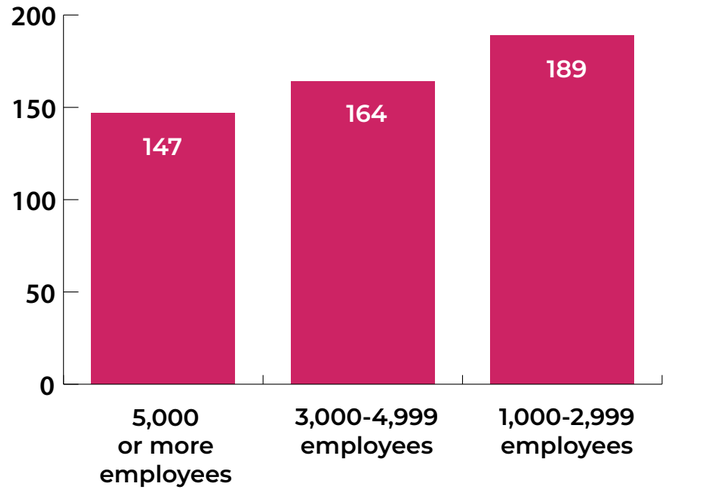
1. In four regions: America, Europe, Middle East, APAC



2. Across a number of sectors: including Finance, Healthcare, Public sector, Energy, Manufacturing etc.



3. Were from organizations with more than 1,000 employees



All interviews were conducted using a rigorous multi-level screening process to ensure only suitable candidates participated.

Qualitative respondents

We conducted eight qualitative interviews with CISOs (or equivalent) in April 2025, split in the following ways:

... by region

In the UK, US and Singapore...


x 4


x 2


x 2

... by organizational sector

- Public sector x 2
- Healthcare x 1
- Financial Services x 1
- Energy x 1
- Manufacturing x 2
- Technology x 1

All interviews were conducted using a rigorous multi-level screening process to ensure only suitable candidates participated.

Section 1

Evolving tactics, familiar attacks in the threat landscape

Threat actors aren't reinventing their strategies, they're refining them.

The current cyber threat landscape is fast-paced and ever-evolving, offering little respite for CISOs as they work to stay ahead of emerging risks. The pressure the majority of CISOs face is evident, with almost all organizations (98%) having experienced a cyberattack in the last year. The threats aren't going away and only add to the burden placed on CISOs, which we explored in last year's report Mind of the CISO: CISO Crossroads, exploring the impact of cybersecurity regulations on the CISO role and their interactions and challenges when reporting to their organization's board.

Past and predicted future risk of cyberattacks

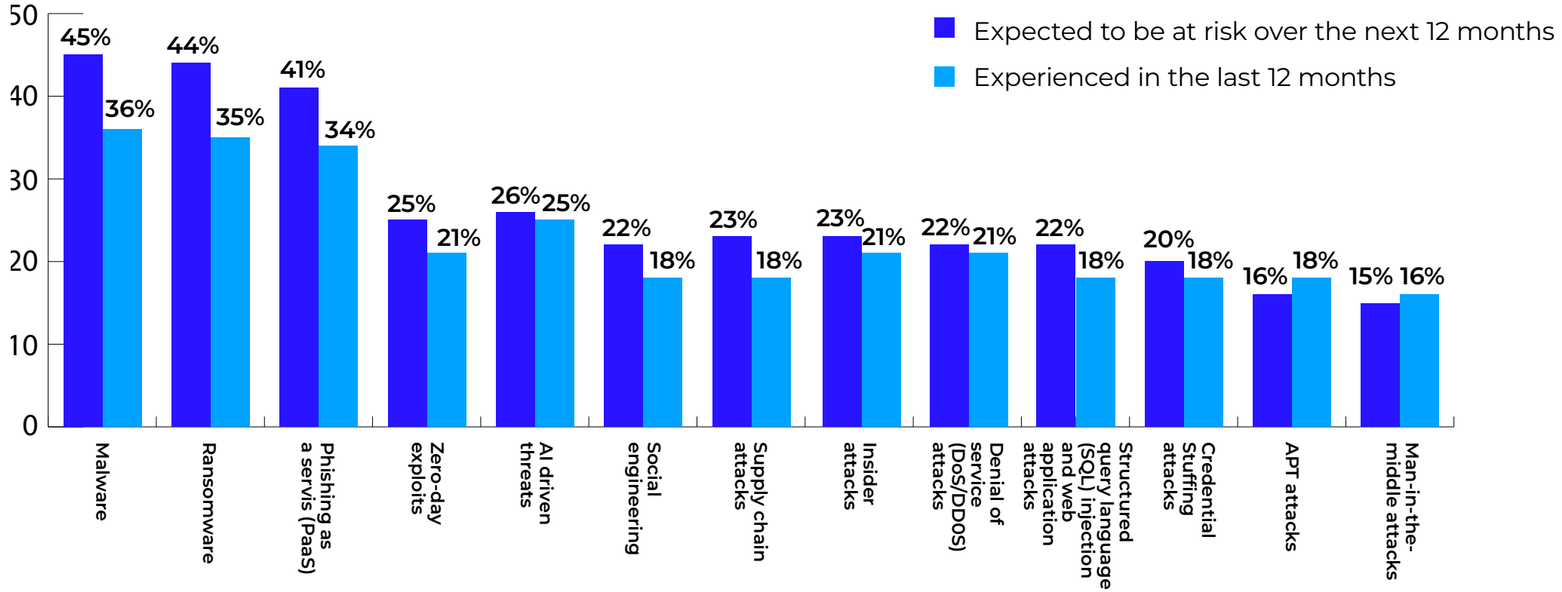


Figure 1. Experienced in the last 12 months: What cyberattacks, if any, has your organization experienced over the last 12 months? [all respondents, n=500] Expected to be a risk over the next 12 months (top three): Which of the following cyber threats, if any, do you believe are the greatest risk to your organization over the next 12 months? [all respondents, n=500]

> **"I would say on high alerts we see a definite increase, an increase in attacks happening every day. Especially since January, we've seen an increase of maybe 25 to 30% in just the daily attempts to attack our systems. Definitely seen increases in different flavors of attempted malware, through email, text messaging."**
>
> – US, Government

> **"... when I say new things it's more of a new techniques, new tactics, new procedures of the same things. I think the threat types we see has not changed a lot ... it's still ransomware, it's still data leakages, data breaches. They all remain the same, but the way they have done it I think is different."**
>
> – Singapore, Technology

Section 1

Evolving tactics, familiar attacks in the threat landscape

Further, CISOs aren't facing unfamiliar threats, but rather evolving ones. Malware, ransomware, and phishing as a service (PaaS) were the most common cyberattacks experienced over the last twelve months, and they remain the major concerns for CISOs when looking forward to the next twelve months.

Even for those who've dealt with these kinds of attacks before, past experiences don't offer much reassurance. Cyber threats are constantly changing, and with AI advancing so quickly, attackers can sharpen their tactics faster than ever. CISOs are left trying to keep pace, often feeling like they're playing catch-up while cybercriminals stay one step ahead. CISOs need effective threat intelligence tools to help them manage these evolving threats.

"... With the advent of AI out there helping to improve the quality of a lot of these phishing emails, it's becoming hard and harder for humans, no matter how well you train them, to figure out if a particular email is malicious or not."

– US, Manufacturing

Another emerging challenge for CISOs is the increasingly blurred distinction between these cybercriminals and nation-state actors. Once separate entities with clearly defined objectives, namely financial gain versus geopolitical advantage, these groups are now adopting overlapping tactics, tools, and technologies such as AI (see Blurring the Lines: How Nation-States and Organized Cybercriminals Are Becoming Alike). As a result, it is becoming more difficult for CISOs to attribute attacks to a specific group and respond accordingly. This convergence highlights the need for proactive threat intelligence. In this evolving landscape, nation-state activity continues to be a major influence on cybersecurity strategy.

Spotlight on ransomware

Consistent with last year's Mind of the CISO Behind the Breach findings, ransomware remains a critical issue CISOs need support with. Over 9 in 10 (93%) agree ransomware is a serious concern, emphasizing the priority it commands within organization's cybersecurity agendas. In fact, the perceived risk ransomware presents has escalated, with a majority (90%) agreeing it has increased over the past twelve months.

There are several ransomware groups presenting the greatest concern, with around a quarter of CISOs reporting these groups pose the most risk to their organizations: **RansomHub (29%), LockBit3 (26%), KillSec3 (23%), and Medusa (22%).**

"The last couple of years we see a lot more targeted organized crime. So we see a lot more organized groups that have success in the background in performing ransomware attacks especially, I see a lot more ransomware-focused type of attacks. The groups tend to lean toward one thing or the other as far as their specialization. Many of them have moved over to ransomware who were probably not necessarily in that before."

– US, Oil & Gas

Section 1A

Nation States

Concerns surrounding geopolitical tensions directly affect CISOs' cybersecurity budgets and strategy.

Nation-state attacks are making the threat landscape even more complicated, a byproduct of our hyperconnected, globalized world. Cyberattacks now easily cross borders, making them harder to contain and respond to. For CISOs, it means having to navigate technical challenges and geopolitical tensions often way outside their control.

From the perspective of the CISO, around half (53%) believe China is one of the top three nation-state threats to their organization. This was far beyond any other country, with the second being Russia, in which less than a quarter (22%) consider the country a top threat.

89%

are frequently asked about nation-state threats by their organization's CEO/board

87%

agree their organization's cybersecurity strategy is influenced by geopolitical tensions such as nation-state threats

85%

agree their organization's cybersecurity budget is influenced by the volume of nation-state threats

CISOs are increasingly focused on addressing nation-state threats, with a growing interest and concern expressed at the board level. A vast majority of CISOs (89%) are frequently asked about nation-state threats by their CEO and/or the board. This interest can have great implications for the organization's cybersecurity strategy and budget. They have substantial authority in strategy discussions, with over four-fifths of CISOs (87%) claiming geopolitical tensions influence their cybersecurity strategy. These threats have an even further-reaching sway as a majority of CISOs (85%) agreed their organization's cybersecurity budget is influenced by the volume of nation-state threats.

There are indications CISOs are growing increasingly fatigued by these threats, calling for a more level playing field. Over four-fifths (85%) believe those within the private sector should be allowed to 'hack back' in retaliation, which triggers an important discussion topic: is retaliating the only fair solution, or will it exacerbate tensions further?

Pressure mounts on healthcare and the public sector

Nation-state threats are of particular concern to those working in the public sector. In fact, nine in 10 CISOs (90%) from this sector state they are concerned cyberattacks on partner nations could serve as a gateway to attacks on their own government and/or critical infrastructure — further highlighting the difficult circumstances many CISOs find themselves in, and the need for comprehensive threat intelligence.

Interestingly, those in the healthcare industry are most likely to be asked about nation-state threats by their organization's CEO/board (97% versus 89% average). This could explain why this sector is the most likely to agree organizations in the private sector should be give the authority to legally 'hack back' cyber attackers (including nation-state actors) (92% versus 85% average). These findings suggest frequent discussions around nation-state threats may be contributing to CISO fatigue and encouraging them to take more drastic actions to relieve pressures from these threats.

> **"We are … a petroleum type company which is a good target for ransomware … Those are the two big ones that concern my company the most, China and Russia."**
>
> – US, Oil & Gas

Section 2

The need for and challenge of operational threat intelligence

Many CISOs struggle with utilizing and integrating threat intelligence to its full potential, unable to take their cybersecurity from reactive to proactive.

As threat actors become more sophisticated and broaden their reach, strong threat intelligence is more important than ever. However, acknowledging its value is one thing – embedding it into a cohesive cybersecurity strategy is another.

Today, CISOs use threat intelligence to train security teams and increase awareness (51%), inform security policy and risk management (48%), and purchase/utilize threat intelligence feeds for blocking and detection. And while valuable, these largely represent tactical or operational use, focused on immediate response rather than long-term strategic planning.

Current use of threat intelligence

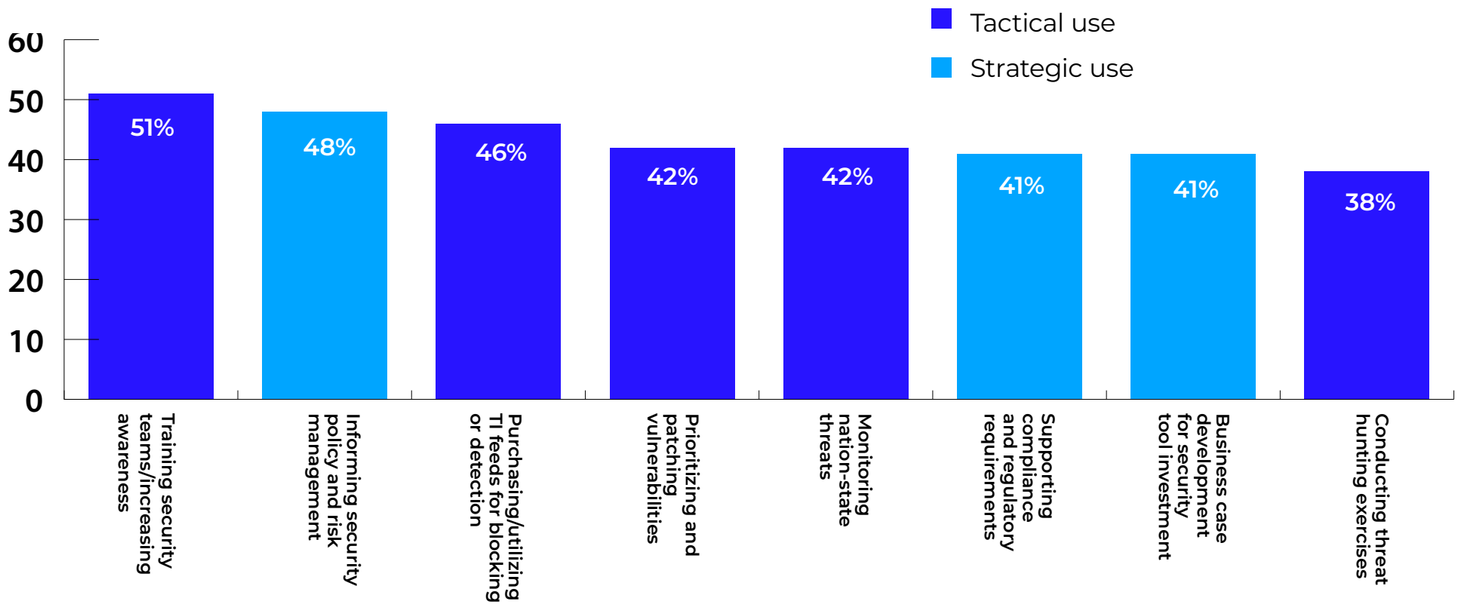
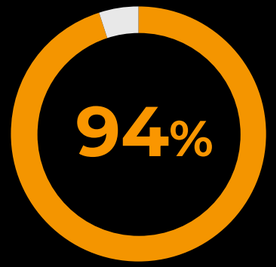


Figure 2. How does your organization use threat intelligence as part of its cybersecurity program? [500]



agree threat intelligence is essential for identifying and mitigating emerging cybersecurity threats

> **"I've always found it difficult to make sure we can actually take advantage of a threat intel feed."**
>
> – US, Manufacturing

Section 2

The need for and challenge of operational threat intelligence

This limited strategic use isn't just a matter of mindset; it results from real, persistent challenges. Threat intelligence may be valued, but acting on it is difficult: **nearly all (98%) CISOs report their organization faces barriers when acting on threat intelligence.**

Organizations are facing a combination of external pressures and internal limitations, with top challenges including keeping pace with evolving threats (45%), integration issues (39%), and regulatory constraints (38%). As a result, threat intelligence often functions in isolation - a reactive layer added to existing workflows, rather than a fully embedded, strategic capability.

Actual strategic value can only be unlocked when threat intelligence is woven into the fabric of cybersecurity operations, not just a standalone input or afterthought. Despite its importance, 60% of organizations have not fully integrated threat intelligence into their cybersecurity strategy – a gap shaped by not only internal limitations, but external forces as well.

Chief among these are policy and regulatory environments, which heavily influence how effectively organizations can operationalize threat intelligence. Yet current legislation and public-sector frameworks often lag behind the pace of evolving threats. For example, in the United States, the 2015 Cyber Threat Information Sharing Act - currently under review - offers a timely opportunity for modernization. Updates should support richer, more contextual, and finer-grained intelligence sharing between public and private sectors, enabling more precise and proactive responses.

For many, threat intelligence use is siloed - used in isolation by specific teams or tools, making it harder to share insights across the organization, coordinate responses, and align security actions.

So, what needs to change? And what do CISOs want to see happen next?

Rebuilding the threat intelligence lifecycle

CISOs are clear-eyed about the road ahead. They recognize modernizing the threat intelligence lifecycle requires significant investment and structural change. In fact, around eight in 10 believe each stage of the threat intelligence lifecycle requires significant improvement or a complete overhaul.

What challenges, if any, does your organization face when acting on threat intelligence?

45%

Keeping up with the evolving threat landscape

39%

Integration

38%

Regulatory and compliance barriers

Section 2

The need for and challenge of operational threat intelligence

This is not about marginal gains. It's about rebuilding the foundations so threat intelligence becomes embedded in how the entire organization anticipates, prepares for, and mitigates risk.

Areas of the threat intelligence lifecycle that need either a complete overhaul or significant improvements

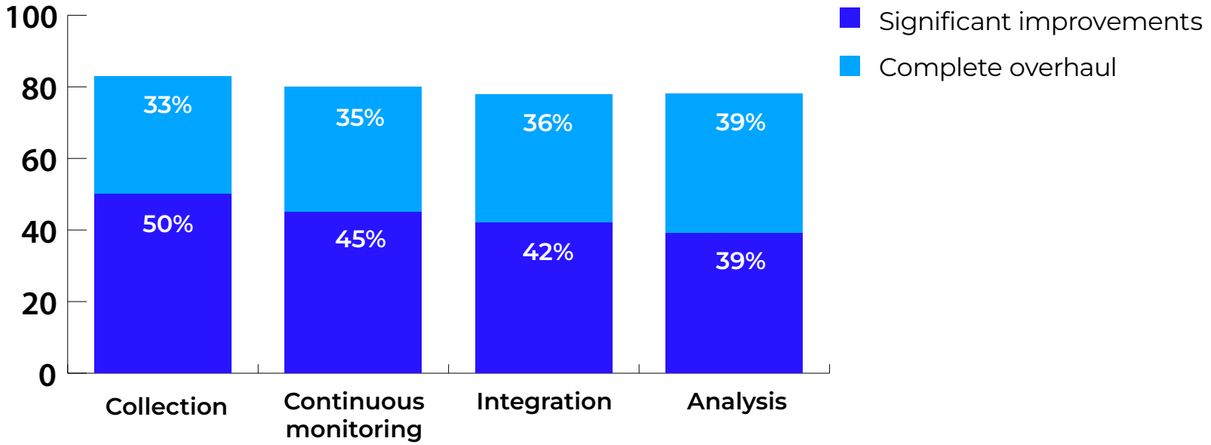
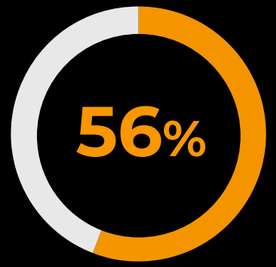


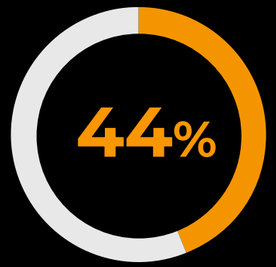
Figure 3. To what extent do the following aspects of your organization's threat intelligence stages need improvement? [500]

To truly unlock its value, threat intelligence must be treated as a central pillar of an organization's cybersecurity strategy. Yet in many cases, its inclusion is reactive – plugging in threat feeds without a clear plan for how or where to apply them. This limits foresight, delays decision-making, and restricts the ability to allocate resources efficiently across prevention, detection, and response efforts.

Proactive applications of cyber threat intelligence (CTI) require a clear understanding of the attack surface and well-defined use cases to ensure intelligence is actionable and effective. Tools such as CTI-CMM and the CREST CTI Maturity Aid can support organizations, especially those newer to implementation, in assessing their current maturity and identifying opportunities to embed intelligence more strategically. Because after all, without a shift towards a proactive mindset, even the most advanced tools risk becoming underutilized.



of organizations are taking a **reactive approach** to using threat intelligence for cybersecurity purposes.



of organizations are taking a **proactive approach** to using threat intelligence for cybersecurity purposes.

Section 2

The need for and challenge of operational threat intelligence

The contrast between those taking a proactive and reactive approach is telling. Over the next 12 months, organizations with a proactive approach are considerably more likely to use advanced threat detection technologies. In comparison, those with a reactive mindset lag behind in every category. This highlights a stark truth - a forward-leaning approach directly influences technology decisions, and by extension, resilience.

Planning to use for threat intelligence over the next 12 months

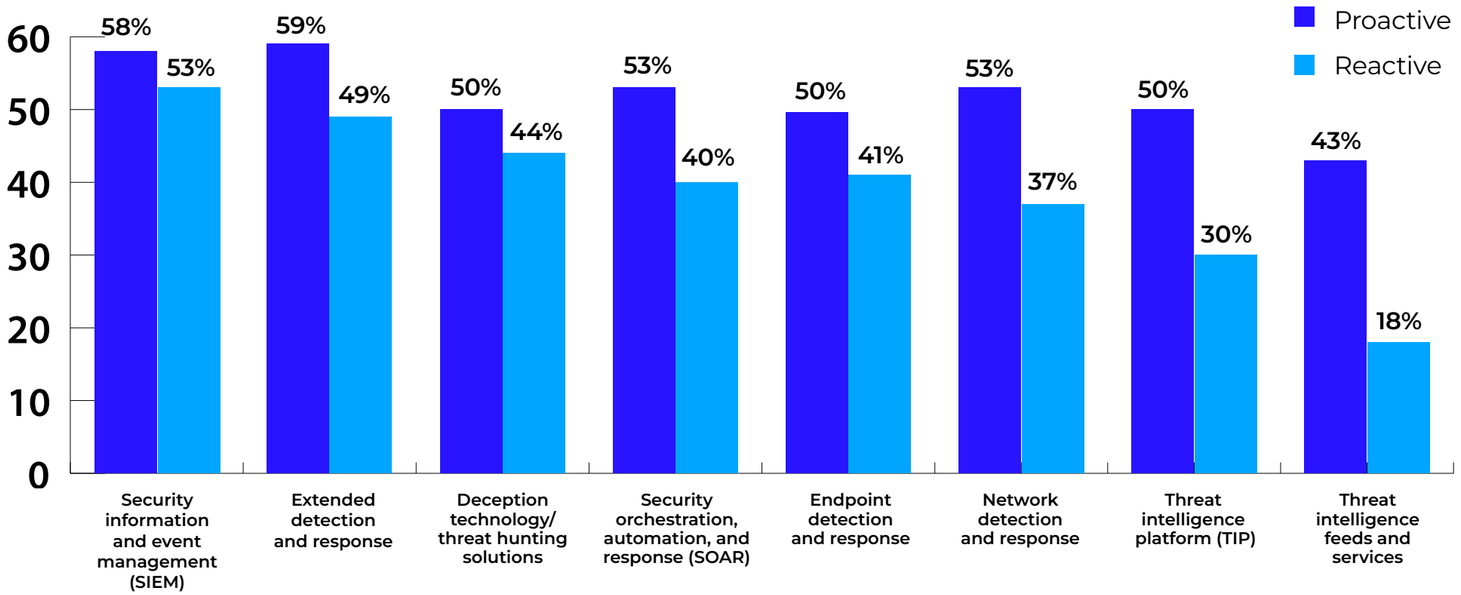


Figure 4. Which of the following does your organization currently use or plan to use for threat intelligence (TI)? - Planning to use in the next 12 months [499], split by proactive and reactive approaches to using threat intelligence for cybersecurity purposes

Ultimately, being proactive isn't just about future-proofing - it's about readiness. It enables faster, more coordinated responses, informed prioritization, and a clearer view of where risk is emerging, helping CISOs to do their jobs. But shifting to this posture takes more than intent; it requires tools, time, and the ability to translate intelligence into timely action.

This is where automation, AI, and orchestration come in.

Section 3

Modernizing cybersecurity response through AI and automation

Combating AI with AI: Artificial intelligence and automation can help CISOs match the pace of cybercriminals.

The answer to ever more sophisticated AI-driven cyber threats could be the use of AI-driven threat intelligence, using AI against AI. With AI and automation speeding up the pace of cyberattacks, CISOs are under increasing pressure to respond fast. In fact, one in four CISOs (25%) believe AI-driven threats will be among the biggest risks to their organization in the coming year. As these attacks become more common, security teams don't just need to follow their incident response plans to the letter, they need to move fast. Fortunately, AI and automation can help them do so.

AI and automation have become critical tools in the CISOs' cybersecurity arsenal. These tools can help CISOs and their teams detect threats and gather the information needed to quickly take action. AI enhances defense strategies by correlating data and identifying the extent of an attack. Automation complements this in tandem by enabling a more rapid response to the attack with minimal manual intervention. CISOs recognize the value of automation in their fight against cyber threats, with over two in five (42%) already using security orchestration, automation, and response (SOAR), and 46% planning to adopt SOAR within the following year.

> **"AI is something I ask every one of our vendors. How are you implementing AI? How are you taking advantage of all these new AI capabilities? What's your AI roadmap look like and how does that fit in your pipeline? And when can we start seeing some of it or testing it out?"**
>
> – US, Manufacturing

> **"The best time to stop … an attack is … immediately with automated response."**
>
> – US, Healthcare

> **"… in the incident, response is all about speed. And so we're trying to introduce more and more automation … if you have an alert to automatically collect all the right documents and logs, present them to the incident responder so they can quickly assess the situation."**
>
> – US, Manufacturing

Section 3

Modernizing cybersecurity response through AI and automation

Although AI and automation are being recognized as a solution to combat cyber threats, some CISOs do not necessarily have the level of automation and AI-driven analytics they believe they need to effectively perform their jobs. A third of CISOs want AI-driven analytics (33%) and increased levels of automation (37%) to help them perform their responsibilities more effectively. Furthermore, over a quarter (28%) report limited automation as making it difficult to integrate tools into their threat intelligence programs properly. This highlights the need for organizations to invest in AI and automation to optimize their cyber response strategy.

This need for smarter, faster tooling extends beyond individual organizations. Government-led threat intelligence sharing platforms must also evolve, with greater investment in AI and automation to enhance speed, precision, and scalability. Accelerating these efforts will not only improve national preparedness but also enable more timely, contextual, and actionable intelligence sharing with the private sector.

33%

of CISOs believe AI-driven analytics would best help them perform their responsibilities more effectively.

37%

of CISOs believe increased levels of automation would best help them perform their responsibilities more effectively.

In addition to strengthening an organization's security posture, AI and automation can streamline many technical aspects of cybersecurity. As these tools take on more of the operational load, the CISO's role continues to evolve. Today, success depends not only on technical oversight but on the ability to communicate with clarity, influence stakeholders, and foster a culture of security - and it's at this intersection of technology and human leadership the next challenge emerges.

"... AI plays a huge part in our defenses. Every core system we have ... all have generative AI integrated into them. One of the greatest tools for generative AI is cyber because there's millions of records from different sources coming in. And it is fantastic at correlating and finding correlations between data coming from different resources and pulling them together in a single pane of glass."

– US, Local government

Section 4

Challenges in communications and training

Internal communications and cybersecurity training create a point of pressure for CISOs.

When a cyberattack occurs, various parties require tailored communications: staff, customers, suppliers, the board, cyber insurance companies, and law enforcement. CISOs and their team are tasked with effectively communicating with these different stakeholders, adapting their message to the specific needs of each group, which is not always straightforward. While engaging with the board about a cyberattack tends to be relatively simple, internal communications can be challenging.

Interaction with the board in the event of a cyberattack is necessary, with all CISOs (100%) reporting they communicate in some way with them during a cyberattack. These updates tend to be of a strategic nature, with over half (55%) of CISOs providing data breach and compliance information as part of these updates.

89%

agree siloed and/or fragmented communication channels limit their ability to address emerging threats effectively.

In contrast, communicating to the wider organization can be anything but easy for CISOs. Almost nine in 10 (89%) agree siloed and/or fragmented communication channels limit their ability to address emerging threats effectively. The lack of a crisis communication plan may exacerbate these challenges, with only 37% of CISOs reporting their organization has a plan in place. Organizations need to support their CISOs, ensuring the appropriate plans are in place should an attack occur.

However, communication channels and a lack of communication planning are not the sole struggles CISOs face with internal stakeholders. Cybersecurity training throughout the organization is self-reported to have limited effectiveness when it comes to threat prevention. There is a call to have training tailored for specific groups within the organization, as opposed to a 'one-size-fits-all' approach.

"... I would call the training we do today really baseline and sort of minimum ... Where we're going is we're going to identify individual groups like executives, HR, Finance, and give them brief, you know, training ... But it's taking us quite a while to get there."

– US, Healthcare

"... we always evaluate and we integrate the feedback about how fast are we informing people. It's not limited to the board, but it also goes to the various senior management and all the way to the public, even to the government and the regulators ... We also noticed that we could have done slightly better."

– Singapore, Technology

"We are trying to build capabilities that are banging up, in some cases, against our information systems or organizations' desire to not share access privileges outside of their own tower."

– US, Healthcare

Section 4

Challenges in communications and training

“We’re relying more on tools, I would say, than we are the human, what we call here like the human firewall … The training we do for the people to spot these things; we’re definitely relying on tools more.”

– US, Government

In relation to teams outside of the security team, only around half of organizations (55%) deploy cybersecurity awareness training for their employees. In a similar manner, but relating to the security team, a little over half (51%) use threat intelligence for training security teams and increasing cyber-awareness. When considered against the backdrop of the evolving threat landscape, these findings are particularly noteworthy and highlight a critical concern: the apparent lack of widespread cybersecurity training across many organizations.

55%

of organizations deploy cybersecurity awareness training for their employees.

CISOs acknowledge the fault, however, particularly within their security teams. There is demand for upskilling within the security team, with some CISOs showing aspirations for increased funding for certifications and continuous learning of new security tools. As cybersecurity tools become more advanced, especially those incorporating AI and automation, comprehensive training will no longer be optional, but essential.

However, security teams will not only need to develop the skills required to effectively deploy, manage, and interpret the outputs of these tools but also enhance their critical and analytical thinking capabilities. As AI-driven solutions become more embedded in threat detection and response, analysts will increasingly take on the role of AI/security custodians, responsible for evaluating, contextualizing, and making judgment calls on the insights these systems generate. This shift demands a new layer of training to equip teams to confidently bridge human judgment with machine intelligence. At the same time, wider employee training will be almost equally critical, as cyber threats become more sophisticated and harder to detect. This tailored approach to training will become fundamental to a resilient cybersecurity strategy.

“… my peers up in [STATE] and a couple other places that have experienced these level one events, they almost always come back to a lack of budget and funds, a lack of training, and most of the times just a complete lack of planning.”

– US, Government

“We do a very small amount of security awareness training. It’s very, very basic.”

– US, Healthcare

Section 5

CISO communities

Strength in numbers: Why community matters to the modern CISO

Throughout this report, one message has been clear: CISOs are being asked to do more, with greater urgency, and under increasingly complex conditions. The role is no longer just technical - it's strategic. Yet many of today's most pressing challenges can't be solved by tools alone. They require shared experience, honest discussion, and the kind of practical insight that only comes from peers who've faced the same pressures - this is where threat intelligence and CISO communities come in.

CISOs aren't just looking for casual networking or surface-level insights - they want trusted, experience-based guidance to help them navigate the complex realities of their role. From sharing lessons learned during real-world incidents to exchanging feedback on tool performance, these communities provide invaluable, actionable insights from those who've lived it.

Resources of support expected from a CISO community

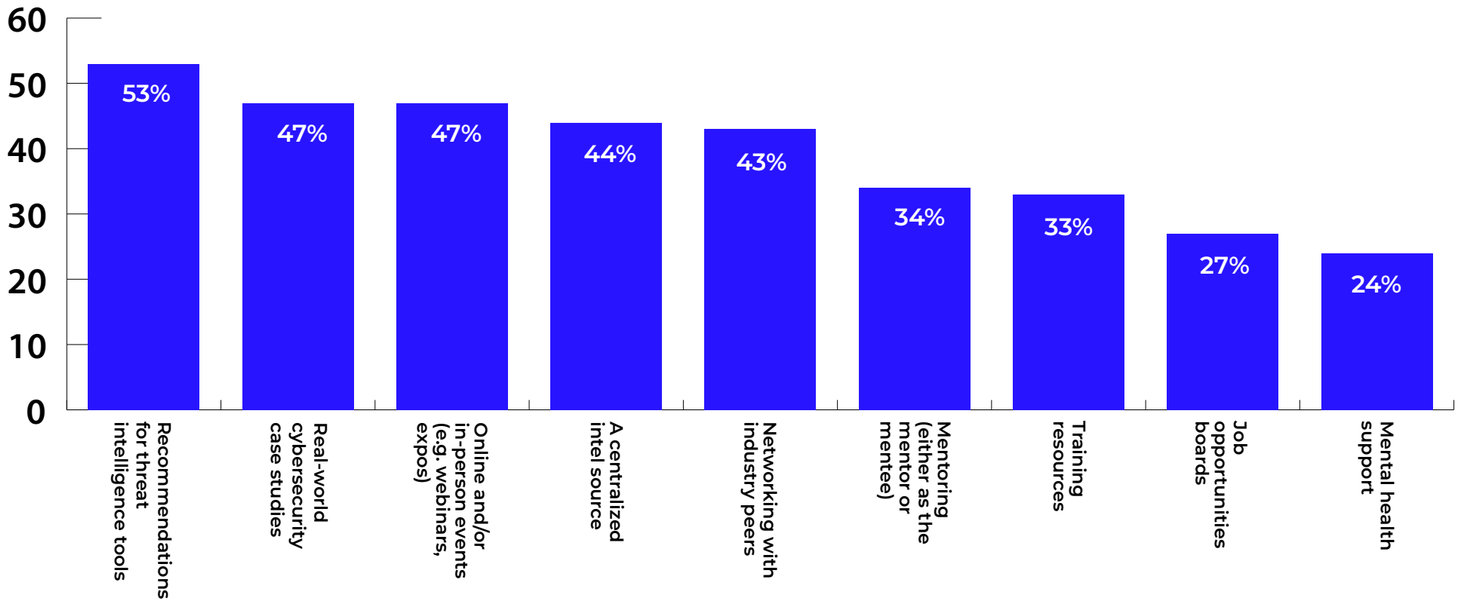
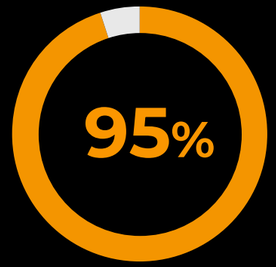


Figure 5. What types of resources or support would you expect from a CISO community, if any? [500]



agree being part of a threat intelligence sharing community or network improves their ability to prepare for threats

Section 5

CISO communities

While nearly all (97%) CISOs are members of threat intelligence sharing communities or networks to some extent, those from proactive organizations are noticeably more engaged. It's a reflection of their mindset - always looking ahead, actively seeking insight, and positioned to leverage intelligence more effectively. By tapping into these networks, proactive CISOs extend their reach, accelerate decision-making, and build resilience through shared knowledge.

Communities and/or networks CISOs are a member of	Proactive approach to using threat intelligence in cybersecurity	Reactive approach to using threat intelligence in cybersecurity
Cyber Threat Alliance (CTA)	52%	33%
Threat Intelligence Exchange (TIE) Platforms	48%	35%
Information Sharing and Analysis Organizations (ISAOs)	44%	36%
Information Sharing and Analysis Centers (ISACs)	45%	33%

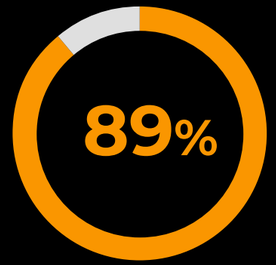
However, participation hinges on trust. Many CISOs are understandably cautious about engaging in large, high-visibility communities where revealing too much could expose organizational vulnerabilities. Without assurances of anonymity and discretion, the risk of open dialogue can outweigh the benefit.

That's why the most effective communities are those built on confidentiality and mutual respect - spaces where CISOs can speak openly, knowing insights will be received in confidence and without judgment.

As organizations work to integrate intelligence, adopt AI, and future-proof their security strategies, CISOs don't need to navigate these challenges alone. The most forward-thinking leaders are already leaning into communities, finding strength in both tools and in each other.

"I just really wish we had communities that were broader where people could actually share their incidents without either A) going to prison or B) discovering that their competitors have just undercut them."

– UK, Government



agree a CISO community would enable security leaders to navigate high-stakes decisions through trusted insights and shared experiences.

Conclusion

The true power of threat intelligence lies not in the volume of data collected, but in how effectively it's applied. For CISOs, the challenge is moving beyond reactive use, making intelligence a core part of their cybersecurity strategy where it informs decisions, shapes policy, and aligns with business risk.

This shift requires more than intent. It calls for a fundamental reframing of threat intelligence - not as a tool for incident response, but as a driver of foresight and proactive decision-making. Yet many organizations still approach intelligence passively, plugging in feeds without a clear understanding of how, where, or when to apply them. Proactive applications of CTI require thoughtful assessment of the attack surface and defined use cases to ensure impact. Without this strategic clarity, even well-resourced programs risk becoming little more than data collection exercises, failing to deliver meaningful security outcomes.

AI and automation can accelerate this evolution by streamlining analysis, surfacing patterns, and enabling faster, more confident action. But smarter tools alone aren't enough. Strategic intent will ultimately define success.

And no CISO should make the shift alone. In an environment where the pressure to act is constant, access to a trusted peer network is invaluable. However, CISO communities offer more than just support - they provide strategic insight, real-world validation, and the space to challenge thinking in ways no tool can. After all, as threat actors grow more coordinated, so too must the defenders. This coordination also raises broader questions, like the widespread support among CISOs for 'hacking back.' While the appetite is clear, this opens up important policy conversations around oversight and the future role of private actors in active defense.

Ultimately, the future of cybersecurity will belong to those who treat threat intelligence not as a function, but as a foundation. This thread connects strategy, technology, and leadership, and the most forward-thinking CISOs are already using it to move from awareness to advantage. For policymakers, this represents a clear mandate: invest in modernizing intelligence sharing frameworks, enable deeper collaboration between public and private sectors, and accelerate AI adoption in national cyber infrastructures. These actions will be critical to ensuring resilience at scale.

Recommendations:

Threat intelligence holds transformative potential, but realizing its value requires structural, strategic, and cultural shifts. CISOs are clear on what's needed: more integrated systems, smarter tooling, and stronger cross-sector collaboration. Governments and industry leaders alike must act with urgency to close the gap between awareness and readiness.

Operationalize threat intelligence as a strategic capability
Organizations must move beyond reactive, siloed applications of threat intelligence. Embedding CTI into cybersecurity strategy requires clearly defined use cases, attack surface assessments, and long-term investment. Adoption of maturity frameworks like CTI-CMM and the CREST CTI Maturity Aid can help guide implementation and support scalable, effective programs.

Invest in automation and AI to close the readiness gap
Many organizations still lack the automation they need to respond to threats at speed. Both public and private sectors should increase investment in AI-driven analytics and orchestration to empower faster decision-making, streamline detection, and enable proactive response.

Strengthen the role of CISO communities
CISO communities are no longer optional. They offer trusted spaces for validation, peer insight, and faster response to evolving threats. Organizations should encourage participation and collaboration across these networks, while industry leaders and security vendors can play a key role in strengthening their impact by supporting confidential, high-value knowledge exchange.

Expand and personalize cybersecurity training across the organization
Upskilling security teams is essential - but so is fostering critical and analytical thinking for analysts tasked with interpreting AI-driven insights. Simultaneously, organizations should implement tailored training programs for wider employee groups to build awareness and reduce exposure to increasingly sophisticated social engineering attacks.

Additional Resources

Mind of the CISO Research Series

- **CISO Crossroads:** Over 500 security leaders worldwide share their views on cybersecurity regulation, the CISO role, and their interactions and challenges when reporting to their organization's board.
- **Decoding the GenAI Impact:** Trellix engaged with 500 security leaders across North America to understand how GenAI and AI are evolving the threat landscape and the CISO role to reshape the future of cybersecurity in the workplace.
- **Behind the Breach:** To shed light on the challenges CISOs face in the aftermath of a breach, Trellix surveyed over 500 security leaders worldwide who have managed a major cyber incident, revealing strategic insights, enlightening stats, and learnings for the best route forward.
- **Understanding the CISO's Struggle:** Trellix engaged with over 500 security leaders to understand what's holding SOC teams back, revealing how they work amidst a tumultuous threat landscape, which business functions hold them back, what tools and support they need to be successful, and how best to move forward.

Trellix Advanced Research Center Digest

Subscribe to get the latest cybersecurity trends, best practices, security vulnerabilities, and more.

The CyberThreat Report: April 2025

Authored by the Trellix Advanced Research Center, this report (1) highlights insights, intelligence, and guidance gleaned from multiple sources of critical data on cybersecurity threats and (2) develops expert, rational, and reasonable interpretations of this data to inform and enable best practices in cyber defense. This edition focuses on data and insights captured primarily between October 1, 2024 - March 31, 2025. Notably this report finds intensification of threats from China and Russia, increased exploitation of vulnerabilities, and cybercriminal voice cloning tools for sale.

Additional Resources

Reporting to the Board: CISO Best Practices
As cybercrime and regulatory pressure on cybersecurity grow, the role of the CISO is evolving from a technical expert to a business-focused leader. Many of today's CISOs are being asked to report to their organization's board on a regular basis. How can you make the most of your time in front of the board? Check out this guide from the Trellix CISO Council to learn best practices for presentations.

The CISO's Guide to Ransomware
When it comes to ransomware, every minute counts. Get road-tested guidance for CISOs and cybersecurity leaders to combat ransomware.

Soulful Work
Cybersecurity provides an opportunity to do meaningful, soulful work. Explore solutions for tackling the cyber talent gap.

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's comprehensive, open and native cybersecurity platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through artificial intelligence, automation, and analytics to empower over 50,000 business and government customers with responsibly architected security.

More at *www.trelllix.com*
Follow Trellix on *LinkedIn* and *X*.

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit *www.vansonbourne.com*