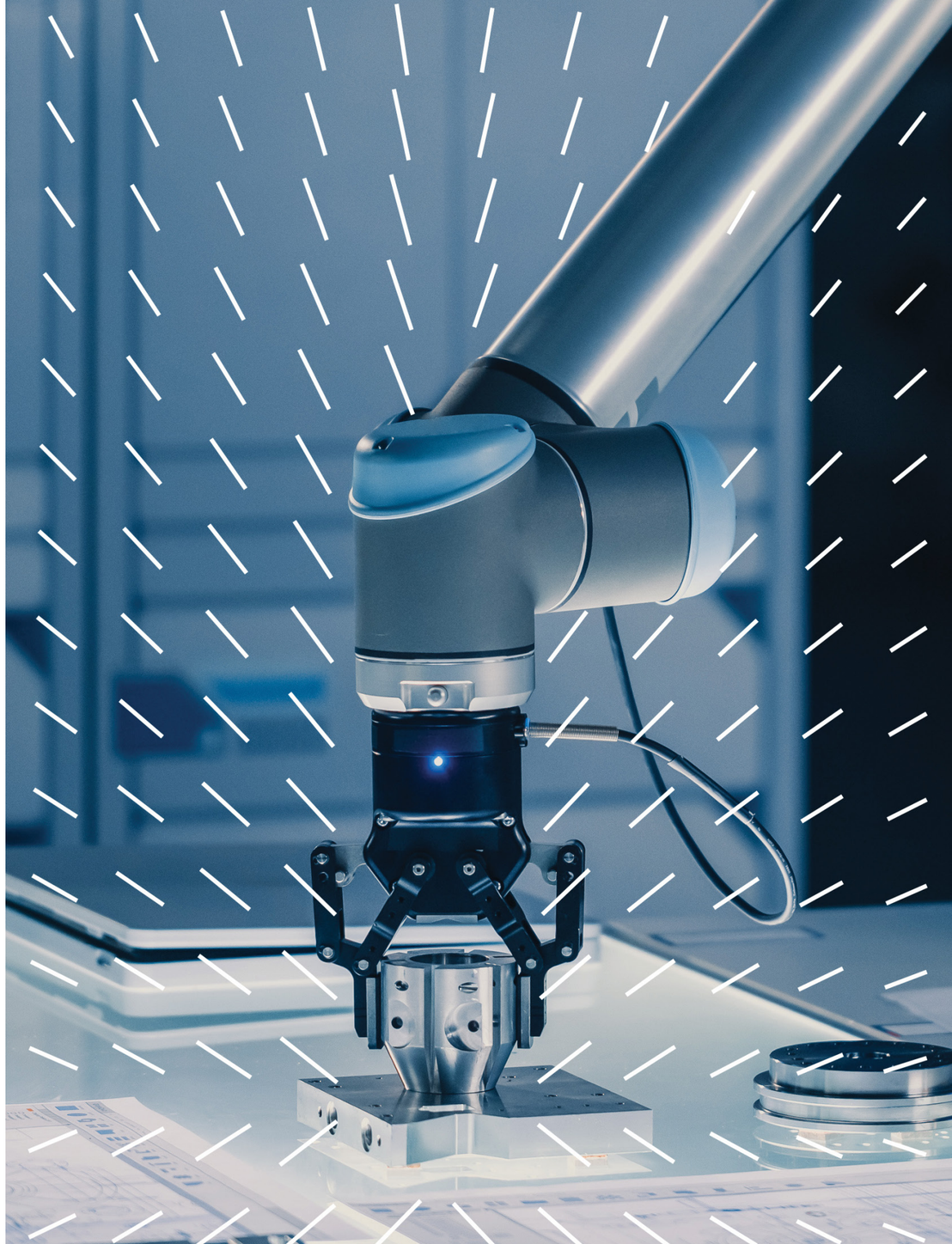
Trellix

# The Mind of the CISO: Behind the Breach

Over 500 security executives share their experience managing a major cybersecurity incident and learnings for the best route forward

# Contents page





# Introduction

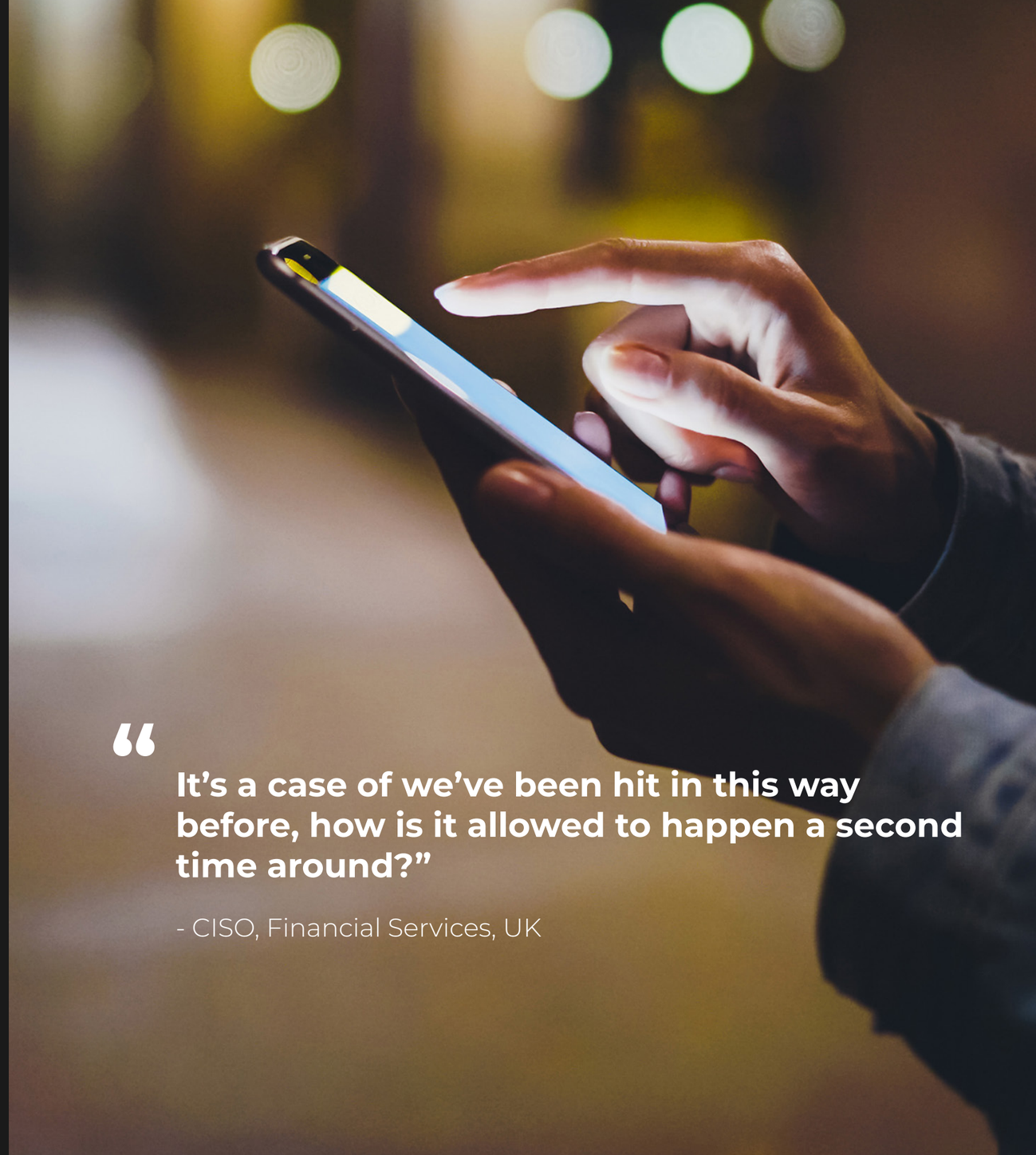
## The CISO’s journey in times of crisis

Entrusted with safeguarding their organizations from cyber threats, Chief Information Security Officers (CISOs) face an ongoing battle.

‘The Mind of the CISO: Behind the Breach’ delves into the intricacies of a CISO’s mindset, exploring their role before, during, and after managing a major cybersecurity incident. We’ll uncover the challenges faced regarding the people, processes, technology, and lessons learned. As we’ll see, the CISO’s journey is one of resilience, adaptation, and resourcefulness to mitigate impacts and evaluate future avoidance.

Trellix, partnering with Vanson Bourne, surveyed and interviewed 512 security leaders from 13 countries who have managed at least one major cybersecurity incident within the past five years, working at organizations ranging from 1,000 to more than 10,000 employees. The industries include energy and utilities, healthcare, public sectors, manufacturing and production, and financial services.

Read on to uncover invaluable insights from cybersecurity leaders after major incidents breach organizational defenses.



> **“It’s a case of we’ve been hit in this way before, how is it allowed to happen a second time around?”**
>
> - CISO, Financial Services, UK

# Key findings

This research reveals critical findings CISOs uncovered in the aftermath of a cyber incident:

**Board support remains critical for CISOs to be proactive in their cyber defense.** With 95% of CISOs receiving more support from their board post-incident, more efficient and effective changes can be made. Increasing budgets for additional tech/tools (46%), rethinking the overall security strategy (42%), and implementing new frameworks and standards (41%) are widespread changes executed, alongside many creating new jobs and responsibilities (38%).

> **“The biggest learning from people is the awareness had to be raised from the board level [...] Unfortunately, it had to take an incident to raise it”**
>
> - CISO, Energy, Australia

**CISOs are facing attacks from all angles.** Data theft attacks (48%), malware (43%), and DDoS attacks (37%) are most commonplace. However, CISOs face the ever-realistic prospect their organization *will* be attacked, and successful attacks are only a matter of time.

**XDR is a viable threat prevention solution.** People, process, and technology improvements are sought by at least 92% of CISOs after experiencing a major cyber incident. 42% say technology not detecting a threat is a cause of the incident, so CISOs are seeking improved technology and support from their vendors. Almost all (95%) believe if XDR was in place, the major cybersecurity incident would have been prevented, demonstrating the impact efficient technology has on SecOps teams and processes.

> **“XDR actually aggregates and correlates data from multiple sources and, therefore, false positives are actually reduced. Alert fatigue [...] is less in the security teams, and XDR also can be proactive in nature rather than defensive [...] which is probably another big difference”**
>
> - CISO, Insurance, UK

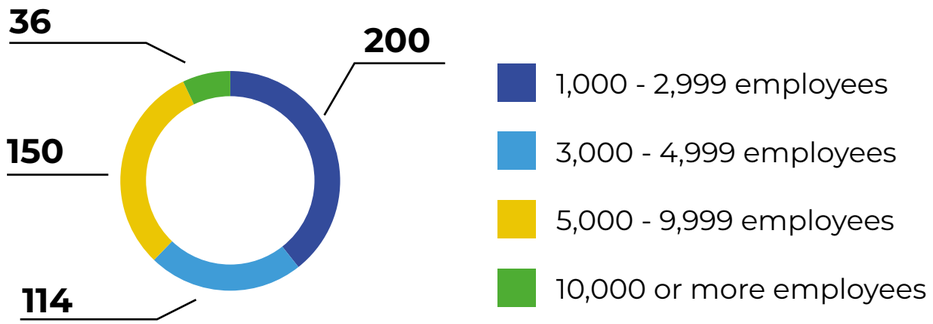
**Impacts to the CISO and their team are evident alongside organizational impacts.** While revenue and customer loss may at first glance be considered top impacts, in reality, data loss (42%) is the most impactful for CISOs. Similarly, significant stress to their SecOps teams (41%) and declining reputation (39%) are further marked concerns, demonstrating areas in which CISOs feel the effects of a major incident the most.

> **“[Experiencing a cyber incident] reinforced the concept we need to be ever-vigilant and no matter how secure we think we’ve gotten things, no matter how many tools we have in place, it’s a constant battle”**
>
> - CISO, Manuafcturing, USA

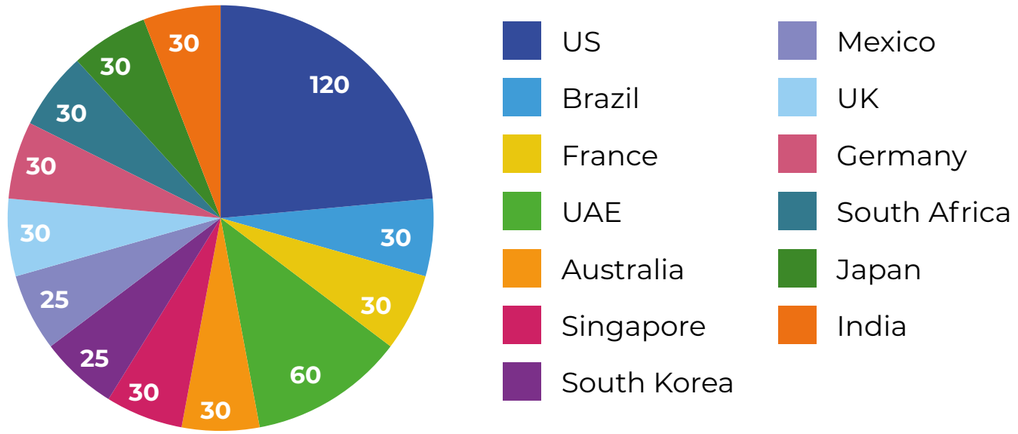
# Quantitative respondents

We conducted a comprehensive survey of 500 CISOs with experience managing a major cybersecurity incident within the past 5 years.

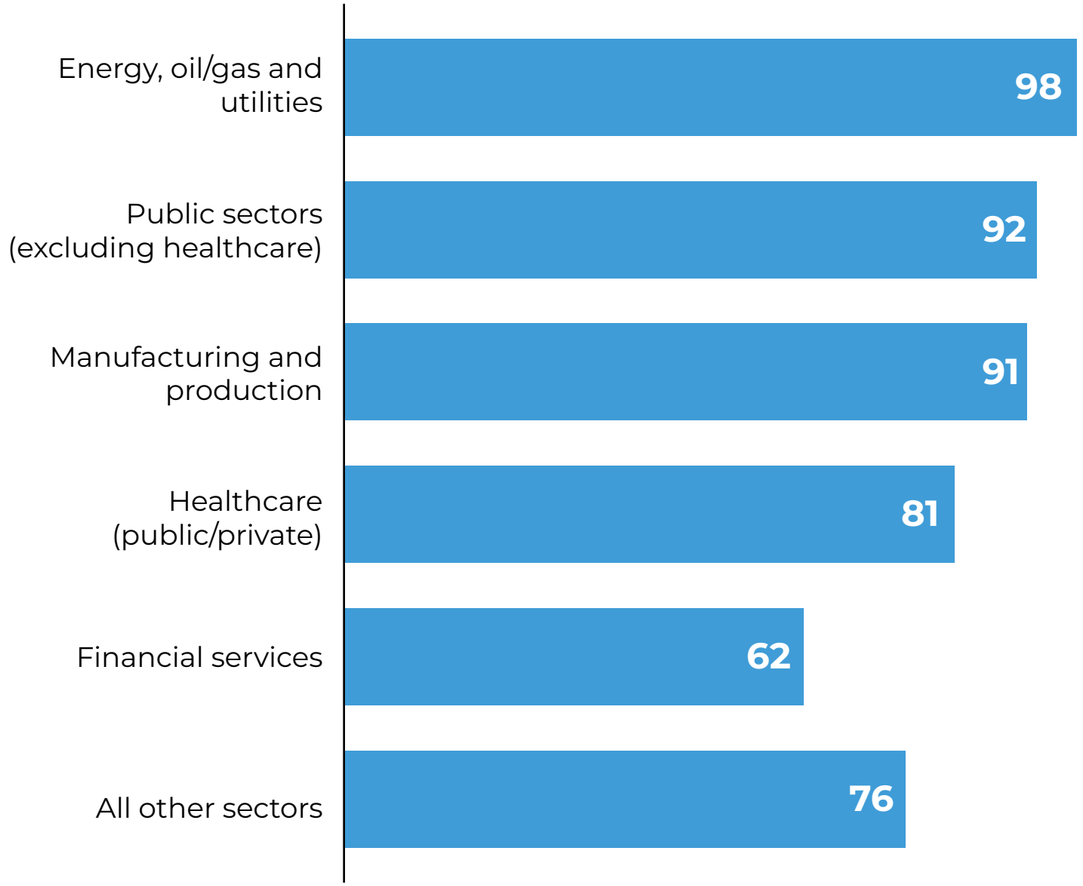
## Organization size




## Country




## Industry

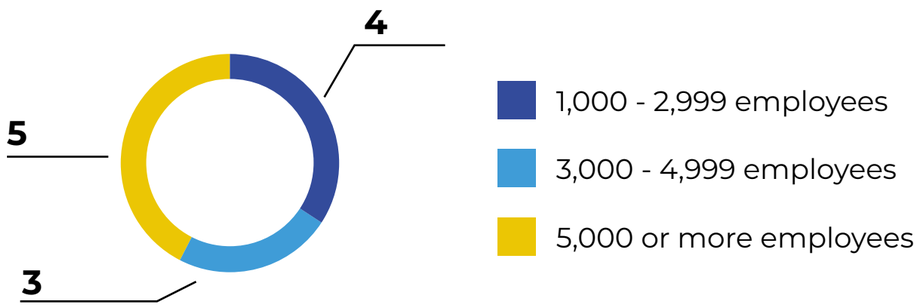



All interviews were conducted using a rigorous multi-level screening process to ensure only suitable candidates participated.

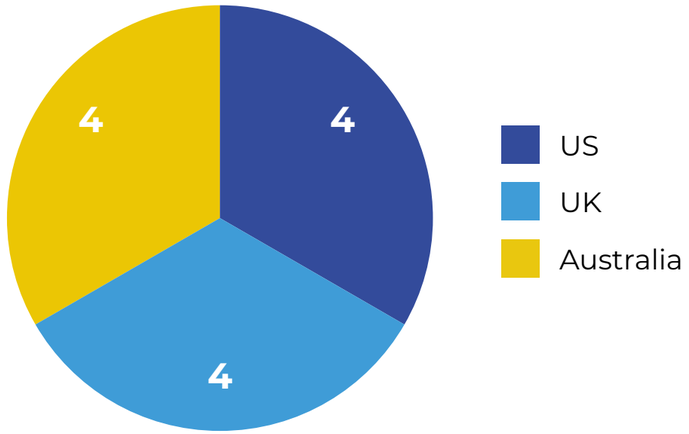
# Qualitative respondents

We conducted in-depth interviews with 12 CISOs (or similar titles) who managed a major cybersecurity incident within the past 5 years.

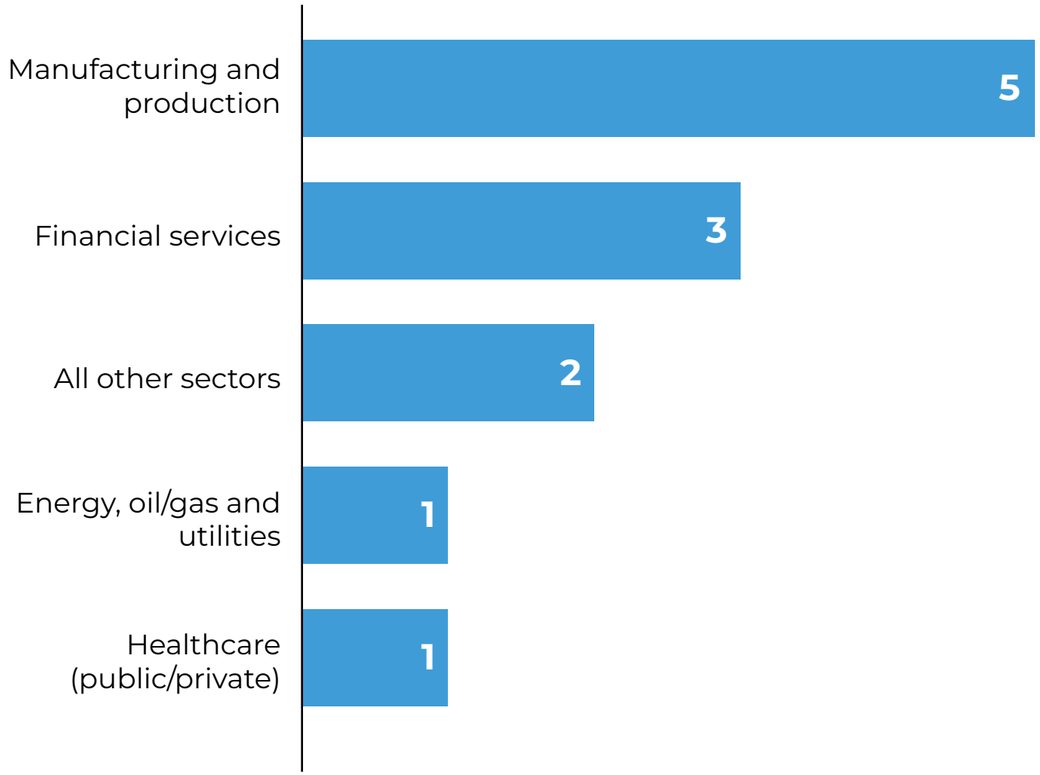
## Organization size




## Country




## Industry




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

Section one

# When a major cybersecurity incident occurs

## What kind of incidents CISOs are facing

In the past five years, CISOs have faced an increasingly sophisticated and diverse range of cyber threats. Most prominent are data theft attacks and malware, closely followed by DDoS attacks, credential stealing, business email compromise, and ransomware, showing cybercriminals are using various attack avenues to infiltrate organizations.

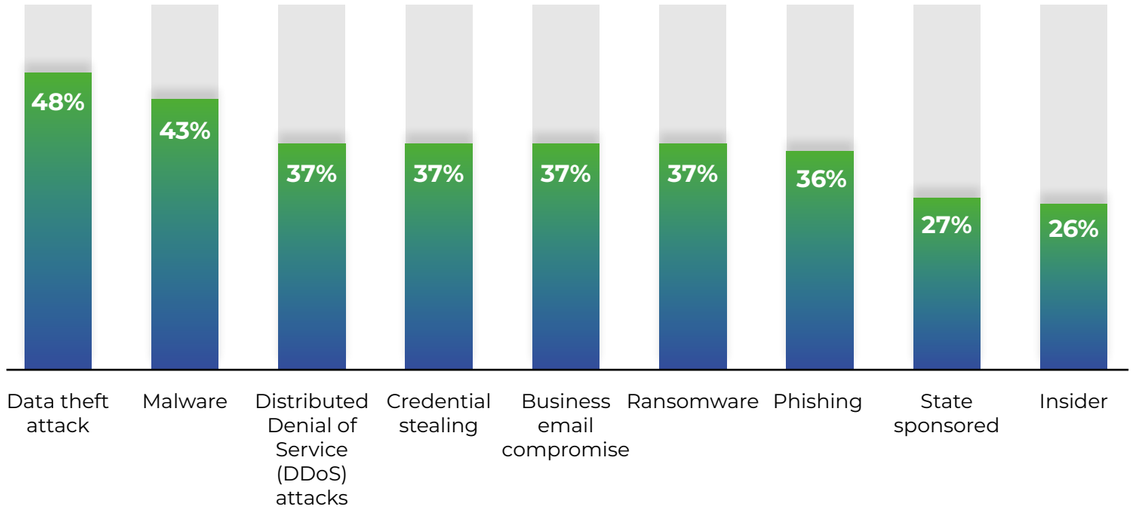



Figure 1. What type of major cybersecurity incident were you involved in managing? [500] Not showing all answer options.

> **“I knew it was a risk constantly and I know the type of security measures in place and they’re decent but again, I also know nation state level actors and organized groups are gonna be able to get past it […] like everybody else, we have limits to our budgets, so there are tools and steps we maybe could’ve taken […] it’s always a balance”**
>
> - CISO, Manufacturing, USA

# How attacks are infiltrating organizations

The primary route in which attackers penetrate organizations' defenses is through the technology they have in place and the inability to detect when threats are present. However, with CISOs selecting an average of 3 causes per incident, it's clear it's not so simple.

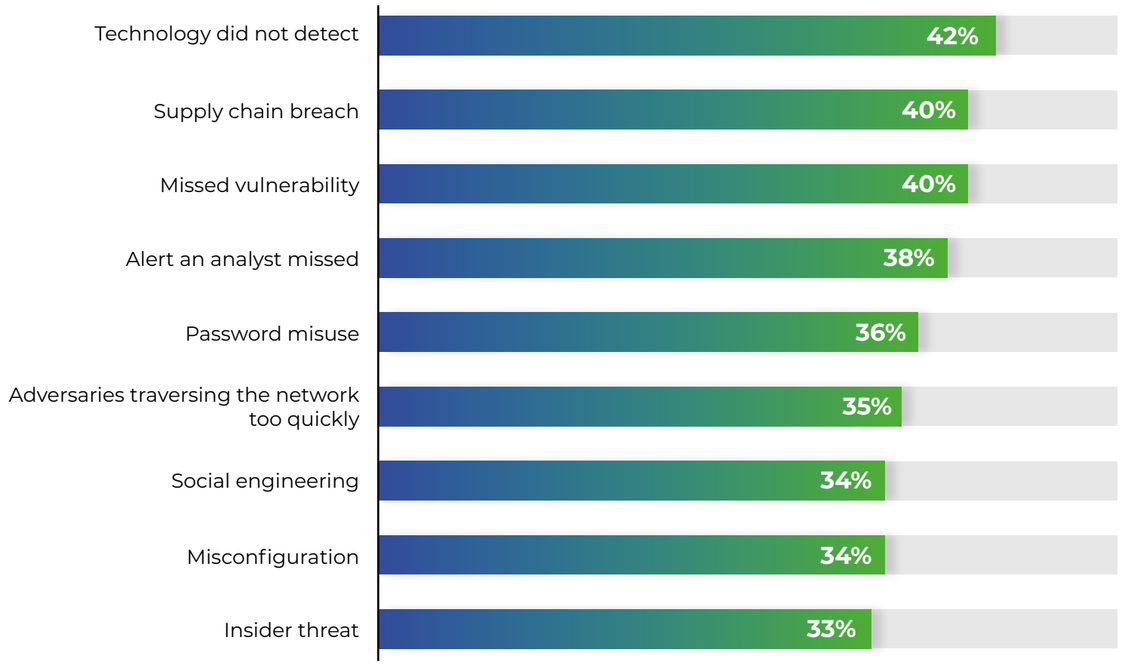



Figure 2. What were the cause(s) of the major cybersecurity incident? [500] Not showing all answer options.

Technology failing to detect was the single root cause for around one in ten CISOs who managed a major incident more than a year ago. The figure more than doubles when looking at incidents occurring in the past year, showing it's increasingly more likely technology cannot keep up with the attacker's ability to penetrate their defenses.

**Root cause of cyber incident: Technology not detecting**


Figure 3. What was the root cause of the major cybersecurity incident? [500] Showing those who selected 'Technology did not detect', split by the incident time frame.

> **"Technology is always vulnerable and while companies have limited budgets, outside there might be unlimited opportunities for hackers"**
>
> - CISO, Insurance, UK

# Is technology implementation giving CISOs what they need?

With a myriad of siloed security solutions making up the framework of their defenses, it's not surprising technologies are at the forefront of blame when it comes to a successful cyber incident.

When the solutions in place aren't combined into a holistic platform, CISOs are taking different approaches and implementing a variety of technologies to bolster their cyber defense – particularly for DLP and MDR.

XDR is reported to be used but also implemented following an incident. However, the understanding of what an open, comprehensive XDR platform is and its true potential to detect, respond, and remediate incidents isn't fully recognized, which we explore on *page 20*.

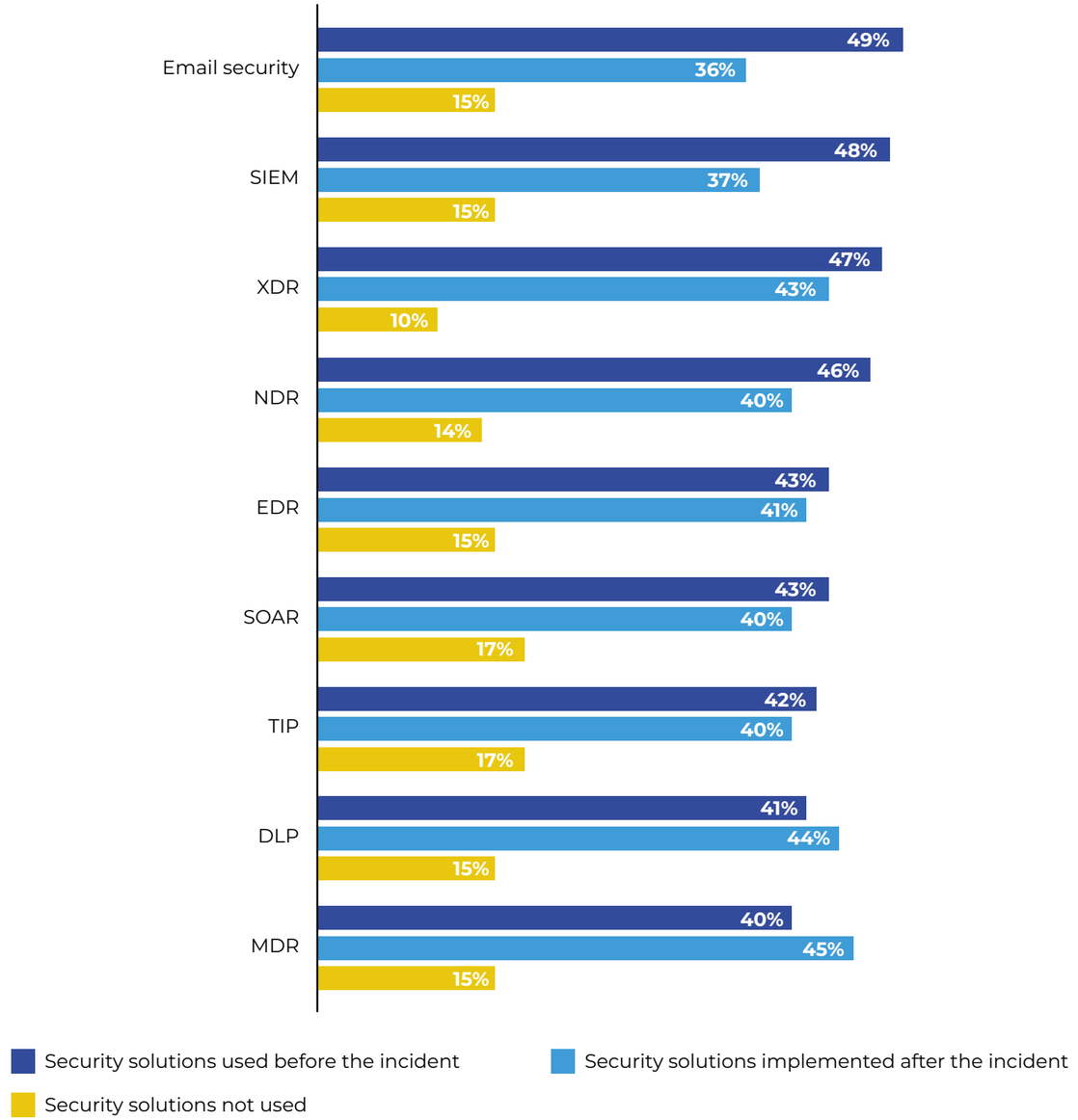



Figure 4. Did the organization use any of the following security solutions before or after the major cybersecurity incident? [500] Not showing all answer options.

## The impacts of a major incident

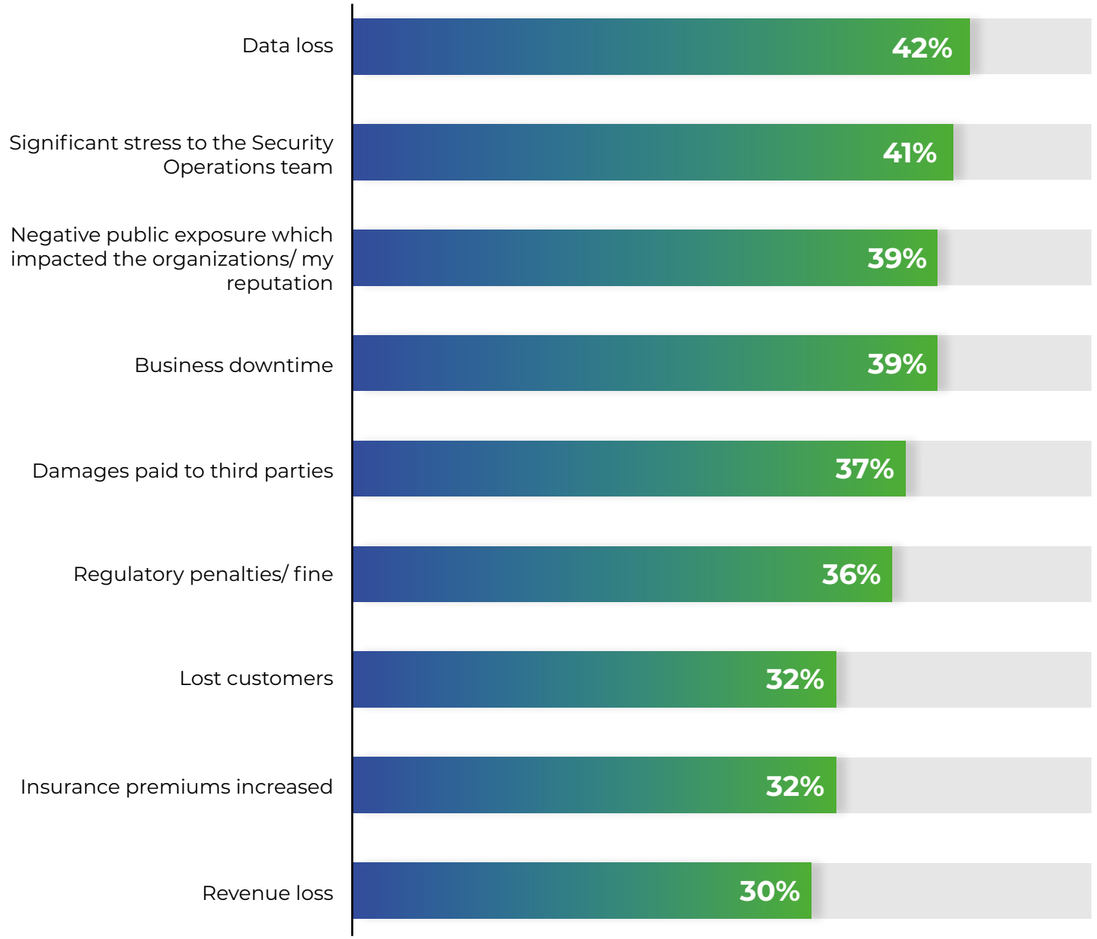



Figure 5. What impact(s) did the major cybersecurity incident you managed have on the organization? [500] Not showing all answer options.

Clearly, CISOs are concerned about losing data. With this often being an organization's most valuable asset, an incident resulting in loss of data through theft or compromise can affect not only an organization's operations but also lead to financial losses as well as damage to reputation.

Second-most to this is the stress levels the Security Operations (SecOps) teams experience during such an incident. Working long hours to detect, respond to, and mitigate the incident, alongside considerable pressure to protect the organization's assets and reputation, is a large concern for CISOs.

Furthermore, reputational damage impacts organizations by eroding trust with customers, partners, and stakeholders, and negative media coverage can affect future customers and revenue.

> **"Just the breach alone cost, with fines and everything, about $6million but with the reputational risk and everything, it was around $25million dollars"**
>
> - Director of Security Operations, Public Healthcare, USA

> **"Even if customers or businesses say, "It's all fine, you handled it very, very well", in the back of their minds, there's always this... how can we rely on this organization? What if it happens again?"**
>
> - CISO, Manufacturing, UK

## The SecOps Revolution

With the rise of sophisticated cyber threats and the need for equally sophisticated technology, *a revolution is rising in the world of SecOps*.

Following the major cybersecurity incident...

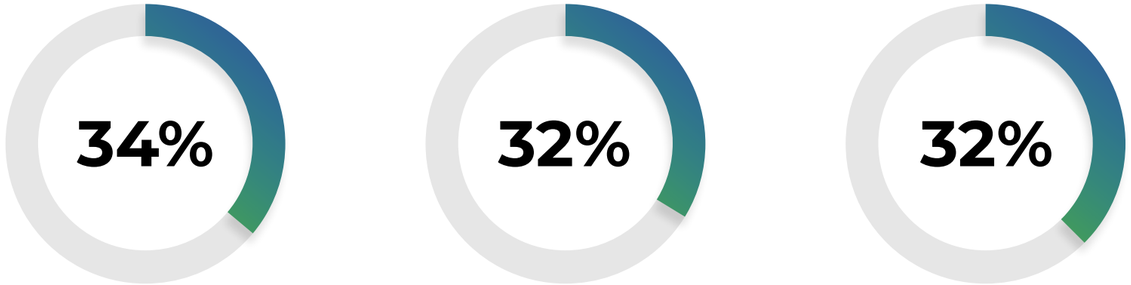



Figure 6. To what extent did your technology, people and processes need to be changed following the major cybersecurity incident? [500]

Over a third of CISOs report the people, processes, and technology needed a complete overhaul, so it's clear their approach to security needs an innovative and proactive change.

The ultimate goal of a resilient security posture means CISOs recognize the need to challenge the status quo and empower their people with next-level tools and capabilities. The threat of AI and its advancements means cybersecurity vendors need to keep pace and innovate, and organizations need to prioritize modernizing their technology and removing legacy systems not serving their current-day needs.

CISOs need to prioritize this too – gaining buy-in from their boards and the financial go-ahead to make such changes, as well as motivating and training their teams.

> **"Again, do you ever really feel like you have everything you need? It's like do you have enough money, do you have a big enough house?"**
>
> - CISO, Manufacturing, USA

> **"There were some cyber-security programs and budgets approved [and we] review[ed] the current state of our technology, people process, technology and data and its security [...] it took a number of years to get there"**
>
> - CISO, Energy, Australia

Section two

# The aftermath of the incident

## Changes to the organization

In the immediate aftermath of an incident, in many cases, it's clear what changes need to be made. In other cases, it takes time for changes to be identified and implemented. CISOs understand the need to be resilient before the next attack and are reliant on their ability to gain board support in order to make the necessary changes. Almost all receive this, with 95% gaining more support following the incident, which is crucial in making the changes identified.

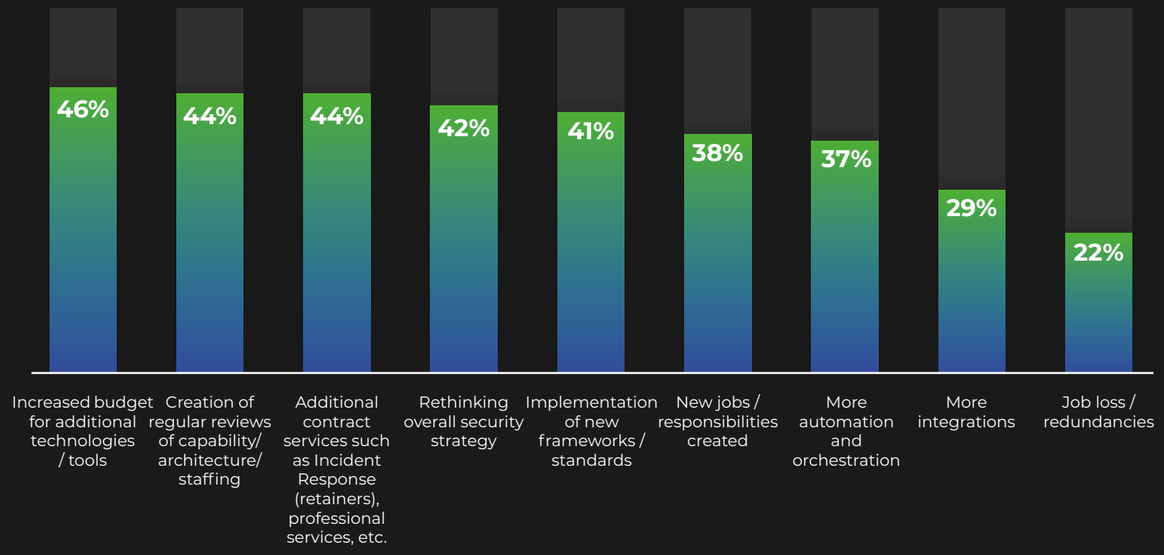



Figure 7. What people, process and technology changes were implemented following the major cybersecurity incident? [500] Not showing all answer options.

Changes such as increasing budgets for additional tools or technologies, or creating capability, architecture, and staffing reviews are immediately impactful events, and these allow some organizations to create new jobs or responsibilities. However, over 1 in 5 organizations experience job losses or redundancies, which seem to be more prevalent for incidents occurring a few years ago (31%) compared to this past year (13%). Perhaps impacts to the team aren't an immediate change following an incident but occur as time passes, when the dust has settled, and CISOs look to restructure or make team overhauls.

**Job losses/redundancies following a major cybersecurity incident**

**31%** More than 3 years ago → **23%** 1-3 years ago → **13%** In the past year

Figure 8. What people, process and technology changes were implemented following the major cybersecurity incident? [500] Showing answers only for Job loss/redundancies, split by the incident time frame.

> **"We wanted to make sure we gave consideration to how we coordinated the response to such situations in a more cohesive manner, what are the strategic lessons learned in relation to the incident"**
>
> - CISO, Insurance, UK

## Changes to the CISO

Managing a major cybersecurity incident is a highly demanding and multifaceted task for a CISO. It involves not only technical expertise but also strong leadership and communications skills, as well as the ability to navigate financial and reputational challenges. And with almost two-thirds (63%) of CISOs we spoke with having managed more than one major cybersecurity incident, it is an inherent part of their role in this digital age.

But why do they stick to this role? At first glance, it looks as though a vast majority of CISOs feel both themselves and their approach to cybersecurity increases in resiliency as time passes. It demonstrates it's not just about preventing incidents for CISOs, but about ensuring the organization can continue to operate, protecting reputation, and adapting to the constantly changing threat landscape.

Further to this, 91% of CISOs report an increase in motivation levels during the incident. Despite an obviously stressful time, an increase in purpose and being able to carry out meaningful, *soulful work* is a clear inspiration for many CISOs.

**Changes to the CISO following the major cybersecurity incident**

**91%** experienced improved resilience as a result of the incident → **91%** report their approach to cybersecurity is more cyber-resilient since the incident → **91%** experienced increased motivation levels during the incident

Figure 9. To what extent do you agree or disagree with the following statements? 'My resilience improved as a result of the incident', 'My approach to cybersecurity is more cyber-resilient since the incident', 'My motivation levels increased during the incident' [500]. Showing combination of those who slightly and strongly agree.

**"Internally I was having my own fears[...] but I was able to protrude a calm mindset most of the time so the team itself doesn't get rattled which was quite important for us"**

- CISO, Financial Services, Australia

**"Personally, I was a bit critical of myself. I was a bit ashamed it happened. However, I couldn't have changed anything, because I have tried my best to communicate my fears"**

- CISO, Energy, Australia

## Changes to the CISO

Following a major incident, CISOs also experienced a change to their overarching views of cybersecurity with a shift towards a ‘never trust, always verify’ approach, which deepens as time passes.

**As a result of the incident, my approach to cybersecurity is ‘never trust, always verify’**

**64%**
In the past year

**82%**
More than 3 years ago

Figure 10. To what extent do you agree or disagree with the following statements? ‘As a result of the incident, my approach to cybersecurity is ‘never trust, always verify’ [500]. Showing a combination of those who slightly and strongly agree, split by the incident time frame.

Zero Trust is most likely to be reported as the single most important framework when managing cybersecurity, yet only a third (33%) of CISOs admit to their organization adhering to the framework at the time of the incident. Clearly, there is a disconnect. Implementing Zero Trust emphasizes a more granular and cautious approach to cybersecurity; therefore, it is not surprising CISOs who have experienced a major incident rank this as highly important.

In the modern threat landscape, implementing Zero Trust architectures and adopting a ‘never trust, always verify’ mindset allows CISOs to help their organizations strengthen their security postures and be better prepared to detect and respond to security incidents promptly.

> **“Always look for the long-term goal as well. A quick win is not always a long-term win”**
>
> - CISO, Manufacturing, UK

> **“You’re never as secure as you would like to think you are, and you have to look in the darkest crevices and the smallest cracks because that’s where the weakness lies”**
>
> - CISO, Manufacturing, USA

## Being a protector and a rescuer

With CISOs demonstrating a stronger commitment to cybersecurity following an incident (91%), it's no surprise to see almost all (95%) change how they describe themselves from before to after the incident.

When asked which descriptive word they most aligned with before the incident, CISOs were more likely to identify themselves as being a 'protector'. And while this remained after the incident, the number of CISOs associating with this definition grew, alongside being a 'rescuer'. Navigating a major incident often leads CISOs to change how they view their role in the organization, and what is needed most of themselves. These experiences often serve as catalysts for growth, and having the duality of proactive ('protector') and reactive ('rescuer') traits can only help a CISO in their preparedness and ability to respond when a future breach arises.

> **"My mindset has[...] shifted slightly from tools to prevention"**
>
> - CISO, Manufacturing, USA

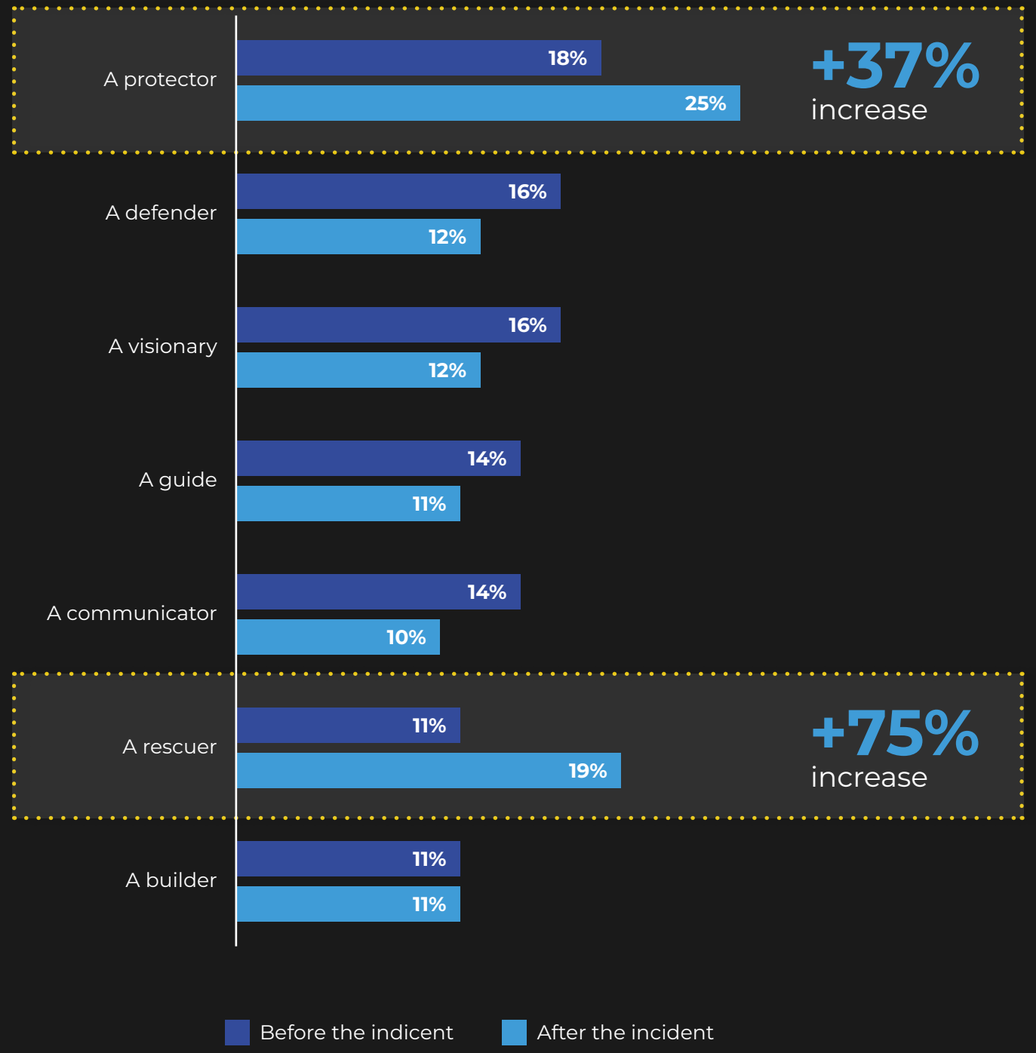



Figure 11. How would you describe yourself before and after the incident? [500] Not showing all answer options.

Section three

# CISOs and their cybersecurity vendors

## The CISOs expectation of cybersecurity vendors

Despite well-formed and often long-term relationships with cybersecurity vendors, a major cybersecurity incident can put even the strongest of relationships to the test. Security vendors are instrumental in defending against known threats; however, it can be impossible to keep pace with the ever-changing attack vectors. So what are CISOs expecting from their vendor during and after an incident?

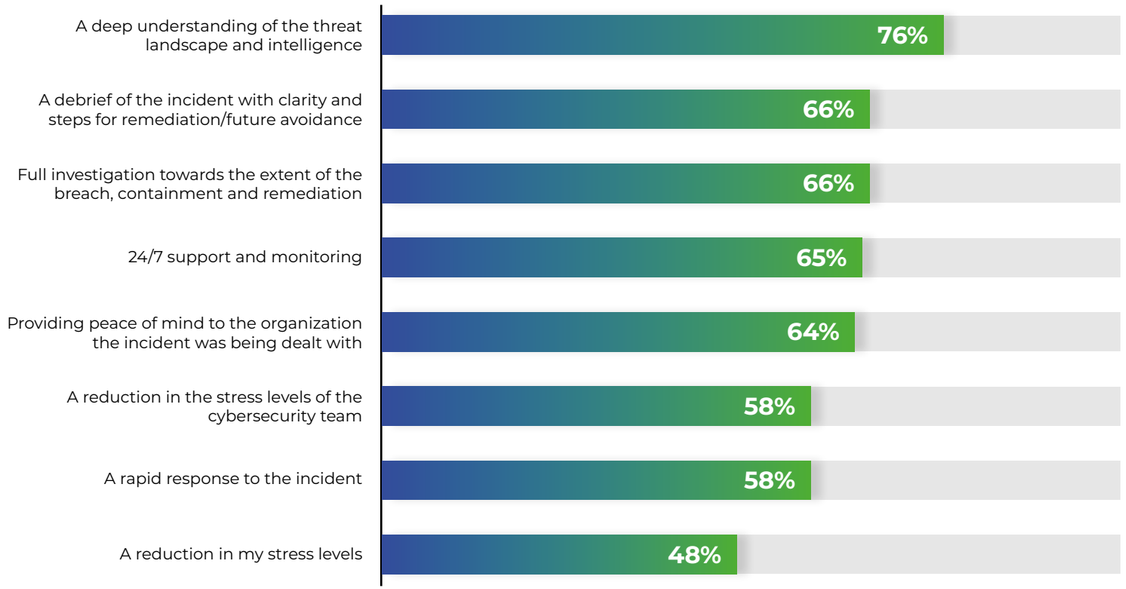



Figure 12. How could the organization's primary security vendor have best helped during and after the incident? [500] A combination of responses ranked first, second, third, fourth, and fifth. Not showing all answer options.

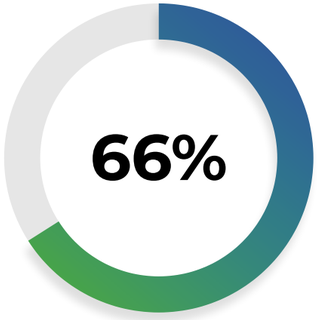
Having knowledge of the threat landscape and being on top of the latest developments, emerging threats, and evolving attack vectors provides CISOs the most peace of mind. Alongside this, of top importance is support from vendors with remediation and debriefing, as well as providing a full investigation into the incident. It's clear, CISOs will look elsewhere for their cybersecurity needs if a vendor fails to provide the expected support (see *page 17*).

> **"I would say in those situations, you often need real-time or near real-time information"**
>
> - CISO, Insurance, UK

> **"I expected them to be joined at the hip with us as we moved forwards because number one, it's what we pay them to do"**
>
> - CIO, Manufacturing, UK

# Vendor loyalty following an incident

Due to failing expectations from vendors during and after the major incident, a majority of CISOs do not remain loyal to their cybersecurity vendors.




**switched or plan to switch** their primary security vendor as a result of the major cybersecurity incident

Figure 13. Did you switch or do you have plans to switch your primary security vendor as a result of the major cybersecurity incident? [500] Not showing all answer options.

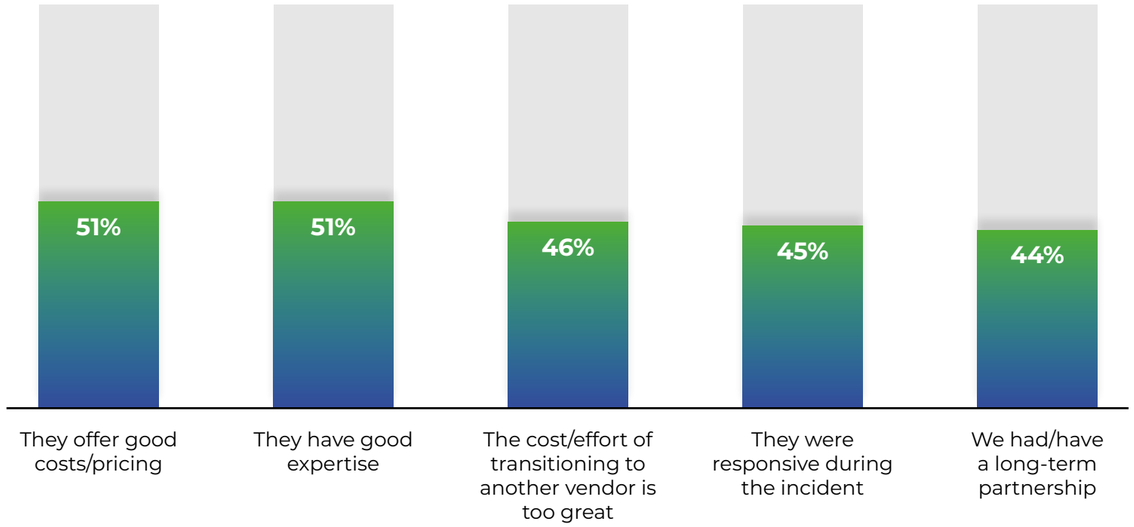



Figure 14. What are the top reasons your organization did not / does not plan to switch primary security vendor as a result of the incident? [169] Asked to respondents whose organizations did not switch primary security vendor as a result of the incident. Not showing all answer options.

With two-thirds (66%) of CISOs either switching or planning to switch as a result of the incident, it demonstrates vendor loyalty is low when an incident occurs. The decision to change or remain with a vendor is a complex one, influenced by a combination of financial, organizational, and strategic considerations.

CISOs consider long-term partnerships as the least important element to consider at this point, displaying pragmatism and a need to demonstrate proactivity in taking action to instill confidence for the board, their customers, and stakeholders. However, if vendors can meet the expectations of CISOs, then they do remain loyal, and relationships are actually strengthened. But it takes working with the right vendor to be in this position.

> **“When the rubber hits the road is where you find out whether or not the money you are paying your security partner is actually worth it”**
>
> - CIO, Manufacturing, UK

Section four

# Learnings from the incident

## People, process, and technology gaps

With a wide variety of cyber incidents experienced over the past five years, CISOs are evaluating contributing factors and lessons learned. Following an incident, CISOs need to consider the people, process, and technology elements and evaluate where changes need to be made.

| | Top reported | Second reported | Third reported |
|---|---|---|---|
| **People gaps** | **46%** Missed due to resource cycles (occurred off-shift, not caught by outsourced) | **46%** Lack of SOC analysts, SOC threat hunters or Incident Responders | **45%** Not enough IT skills to deal with the complexity of the incident **AND** Gap in knowledge meant team was unsure of how to handle |
| **Process gaps** | **53%** Technology limitations / gaps meant process could not be fully executed | **50%** There were too many manual processes which delayed the mean time to detect or repair | **43%** Lack of properly documented and implemented process |
| **Technology gaps** | **45%** The technology was not configured correctly / detection policies were not enabled | **42%** Gap in security capability / technology | **42%** Inability to contain quickly, even after detection **AND** The technologies deployed were not integrated / were siloed |

Figure 15. How did the people/process/technology gaps contribute to the major cybersecurity incident? [500] Showing the top three answer options selected.

Gaps within the people in their organization can be significant, such as missing alerts due to resource cycles or not having the appropriate team in place with a lack of SOC analysts or threat hunters. With the talent gap in cybersecurity approaching 4 million people in 2023 (according to the International Information System Security Certification Consortium - *ISC²*), CISOs need to consider best how to address lacking skills in their organizations, from drawing in new talent to upskilling their current workforce.

> **“The most important asset or factor in IT or security is not the technology, not the policy or process, not the tools, it’s the people. Get the people on board, get the people adopted, get the people understanding and contributing, the other stuff falls into place”**
>
> - CISO, Manufacturing, UK

Technology gaps within an organization significantly contribute to successful cybersecurity breaches by creating vulnerabilities and weaknesses cybercriminals can exploit.

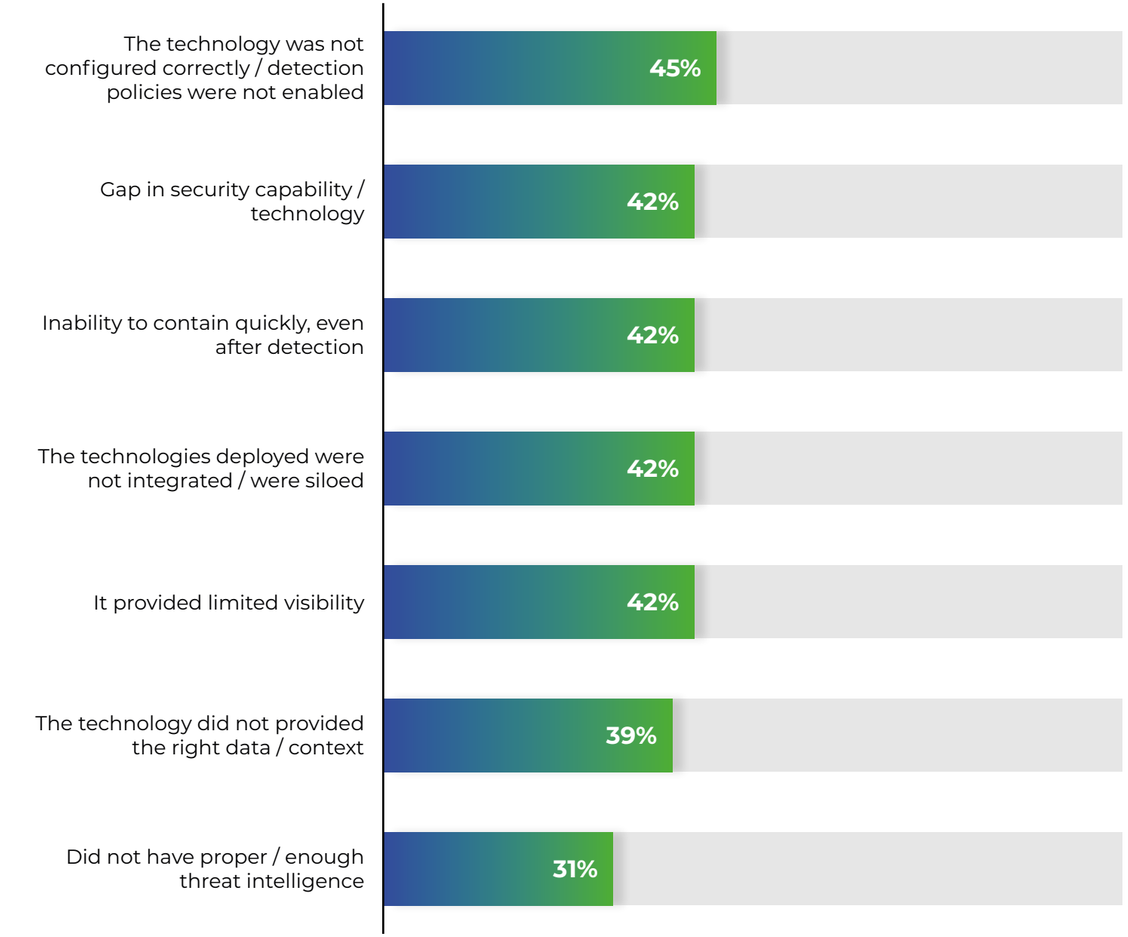



Figure 16. How did the technology gaps contribute to the major cybersecurity incident? [500] Not showing all answer options.

Further to this, technology gaps are also linked to teams being unable to fully execute the processes in place (53%), showing if the technology is not sufficient, the organization's practices and procedures created to protect their organization cannot be completed – leaving further vulnerabilities.

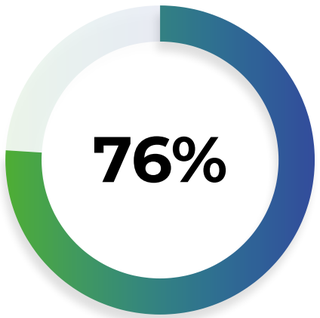
People, process, and technology gaps are all intrinsically tied together and can reinforce or exacerbate smaller gaps. A successful incident often arises when multiple gaps align, and therefore CISOs are aware they must work to address these gaps holistically, promoting a culture of security awareness, refining processes, and deploying up-to-date and effective security technology.

> **"Our [incident] response processes were up to scratch, however the process of managing the communications, process of managing the crisis. There were a lot of gaps identified and therefore we did a post-incident review. We identified lessons to be learned and we have improved our strength in those processes"**
>
> - CISO, Energy, Australia

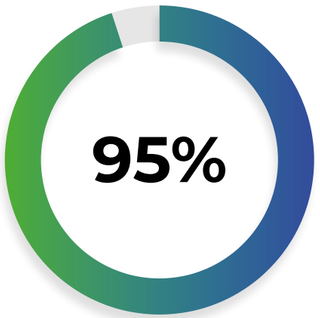
## Are CISOs using XDR?

In the midst of a cyber incident, XDR provides additional visibility and threat detection capabilities to enable organizations to quickly and effectively respond to breaches, as well as investigation and incident resolution capabilities.

CISOs widely agree with these benefits, with over three-quarters believing if they had XDR, their major cybersecurity incident would have had a lesser impact, or would have been prevented entirely.




**agree** if they had XDR, the major cybersecurity incident would have had a lesser impact




**agree** if they had XDR, the major cybersecurity incident would have been prevented

Figure 17. Based on your understanding of XDR as a platform that connects your tools, to what extent do you agree or disagree with the following statements? [500] Answered by respondents whose organizations weren't using XDR at the time of the incident, showing combination of those who strongly and slightly agree. Not showing all answer options.

> **"If we had true correlation across all the tools, would we have caught it earlier?"**
>
> - CISO, Manufacturing, USA

> **"Increased visibility. You know, more information, more data"**
>
> - CISO, Manufacturing, USA

## The benefits of XDR

CISOs look for technology changes following an incident (*page 11*), and must consider which technology is most appropriate to implement. Many consider XDR, with 43% implementing it in the aftermath of an incident. Depending on the root cause of the incident (technology did not detect or a missed vulnerability), CISOs are more likely to seek XDR to solve these areas of weakness.

Supporting this viewpoint are the benefits CISOs look for when considering an XDR solution. Providing better visibility, prioritizing alerts, and providing overall faster and more efficient threat detection and response will allow security teams to stay ahead of cyberattacks while minimizing their impact when they do occur.

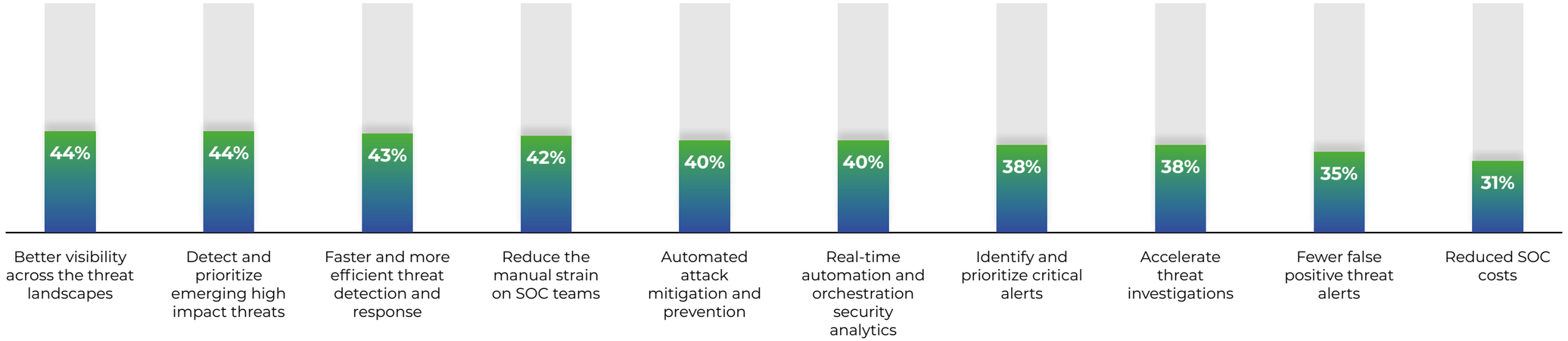



Figure 18. When considering an Extended Detection and Response (XDR) solution, what benefits would you look for it to include? [500]. Not showing all answer options.

> **“I literally have three different monitors sitting in front of me so I can watch as many screens as possible when the time comes. But if I can consolidate everything into a single screen without having to jump into different screens and different graphical designs and whatnot, it really is helpful in terms of number one, getting to know the information visibility, number two, monitoring, number three, enforcement”**
>
> - CISO, Financial Services, Australia

# Conclusion: Building Cyber Resilience

Organizations need to prioritize building cyber resilience to prevent future attacks. This requires significant investment in the right, people, processes, and technology solutions. As made evident in this research, CISOs are in need of additional resources and support, starting at the board level to make the required investments, training, and overhaul needed to keep pace with the evolving threat landscape. New global regulations and legal ramifications in the wake of cyber incidents should help to prioritize the needs of CISOs moving forward, equipping them with the resources to effectively and efficiently manage cyber threats.

### Strengthening Cybersecurity with XDR

Diving deeper into the technology needs of CISOs to build cyber resilience, with technology cited as the number one cause of detection failure for cyber incidents - it's clear organizations urgently need multi-vector detection and faster context to stay ahead of threats. The Trellix XDR Platform shuts down threats with AI-powered speed, because every minute counts when facing a cyber threat. CISOs can transform their security operations and strengthen their organization's cybersecurity posture with:

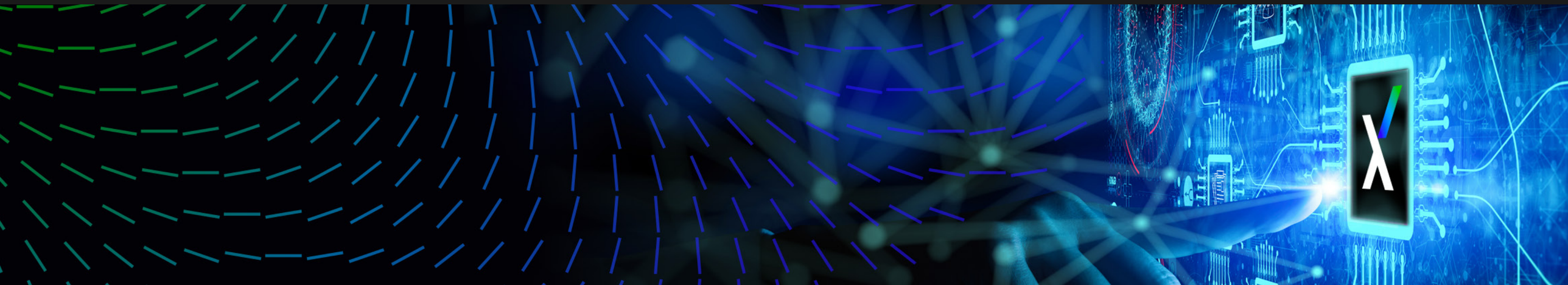
- **Comprehensive native controls:** One platform of best-of-breed tools to replace five or more point products
- **Integrated analyst experience:** Dashboards designed by analysts, for analysts, and playbook automation to enrich data and remediate threats
- **Multi-vector threat detection:** Turn event noise from multiple controls into prioritized, insightful actions
- **Open platform:** More than 500 out-of-the-box integrations for quick time-to-value
- **Actionable threat intelligence:** Operationalize threat intelligence from 1 billion global sensors to produce actionable, real-time insights on emerging threats
- **Future proof investment:** AI-powered, scalable hybrid architecture grows with the environment and as new technologies emerge

Learn more about the *Trellix XDR Platform* today.

> **"You never, never hit that point [prepared as you could be for any sort of incident]. Any time I start thinking I am, then I'm not doing my job."**
>
> - CISO, Manufacturing, USA

# Additional Resources

- *Trellix XDR Platform*: Reduce risk, cost, complexity, and time to value with a single, open, comprehensive AI-powered XDR platform.
- *Soulful Work*: Cybersecurity provides an opportunity to do meaningful, soulful work. Explore solutions for tackling the cyber talent gap and increasing diversity in cybersecurity.
- *Trellix Advanced Research Center Digest*: Subscribe to get the latest cybersecurity trends, best practices, security vulnerabilities, and more.
- *Trellix's Mind of the CISO Research (April 2023)*: To get inside the minds of today's security leaders, Trellix engaged with over 500 CISOs from around the world to understand their struggles and SOC challenges. Dive in now for illuminating stats, real-life quotes, and more.
- *Ransomware Detection and Response Virtual Summit (Watch On-Demand)*: Learn from cybersecurity leaders and CISOs in a panel discussion on best practices to bolster cybersecurity.



Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) 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 machine learning and automation to empower over 40,000 business and government customers with living security. More at *www.trelllix.com*
Follow Trellix on *LinkedIn* and *X*.

VansonBourne

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*