Trellix

2023 REPORT

The mind of the CISO

Over 500 security executives share what's holding SOC teams back—and how to best move forward

Cybersecurity is more nuanced and advanced than ever before. Unfortunately, so are cybercriminals.

As bad actors embrace novel attack methods, security operations (SecOps) teams struggle to find the right processes and tools to detect and respond to emerging threats quickly.

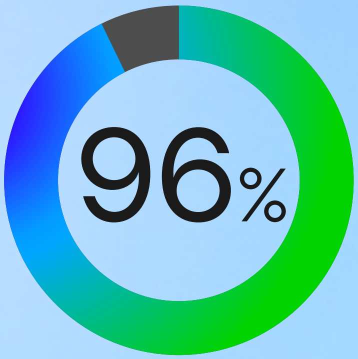
Many organizations rely on legacy technology like SOAR and SIEM—tools that once helped SecOps work more efficiently and effectively. But as cybersecurity became more sophisticated, these solutions became outdated.

Lack of modern technology is only one of the common hurdles for today's security operations center (SOC) as the threat landscape changes.

What are the other major challenges facing today's SOC? And how can organizations evolve to reduce stress on staff while increasing security? No one understands these questions better than chief information security officers (CISOs).

To get to the bottom of what's really going on in today's SOC, Trellix surveyed and interviewed 525 security leaders from around the world. Partnering with Vanson Bourne, we talked to CISOs in 9 countries who work at organizations that range from 1,000 to more than 10,000 employees. We spoke with CISOs who oversee SOC teams in a range of industries, including public sector, healthcare, and financial services.

Read on to see what we uncovered.

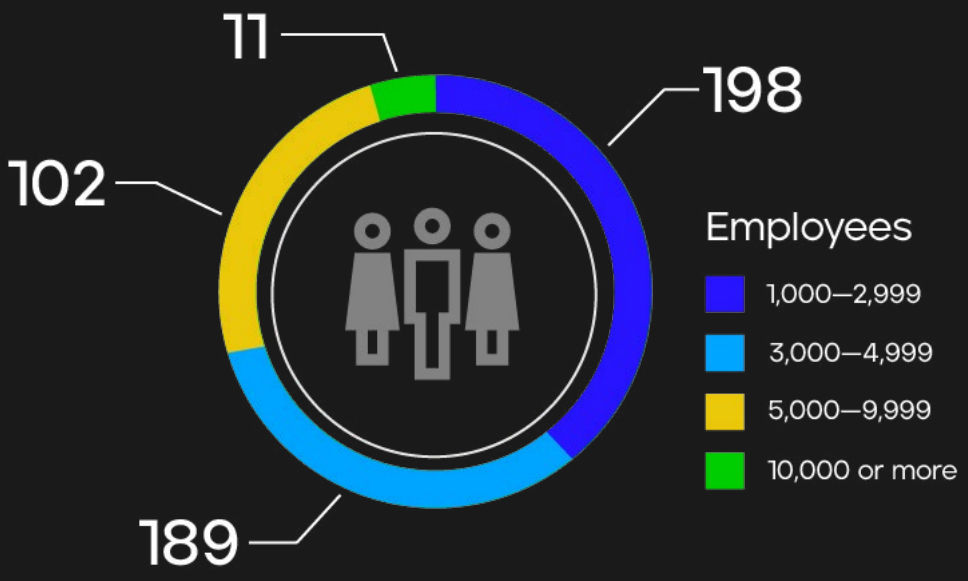


of CISOs say they need better solutions for their organizations to be more cyber resilient

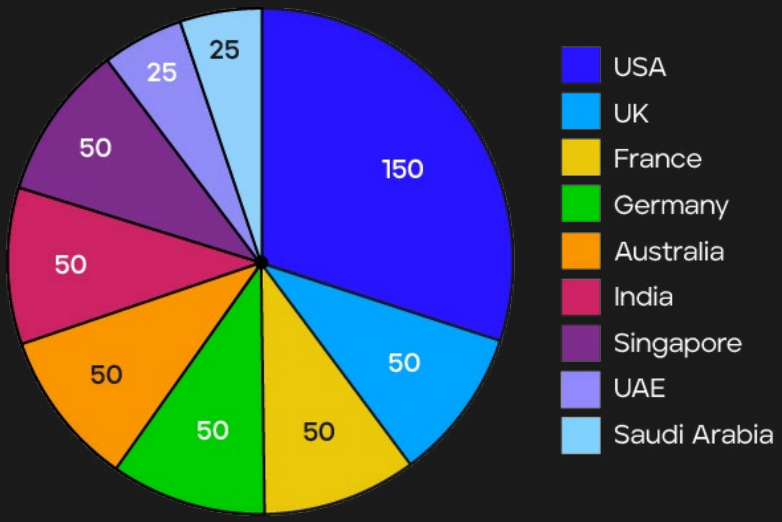
Survey respondents

Quantitative research: We conducted a comprehensive survey of 500 CISOs

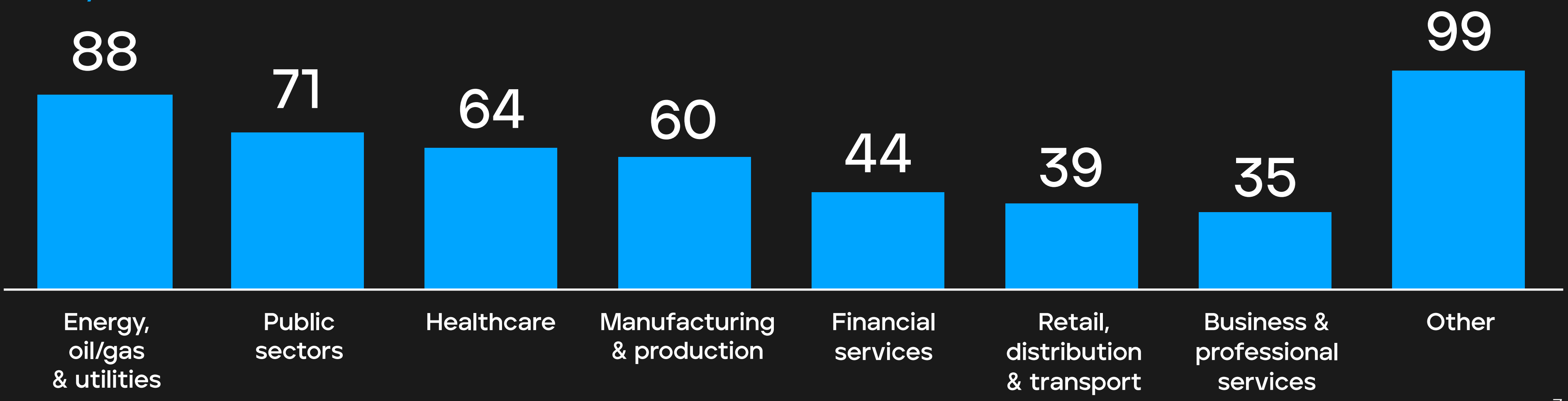
Organization size



Country

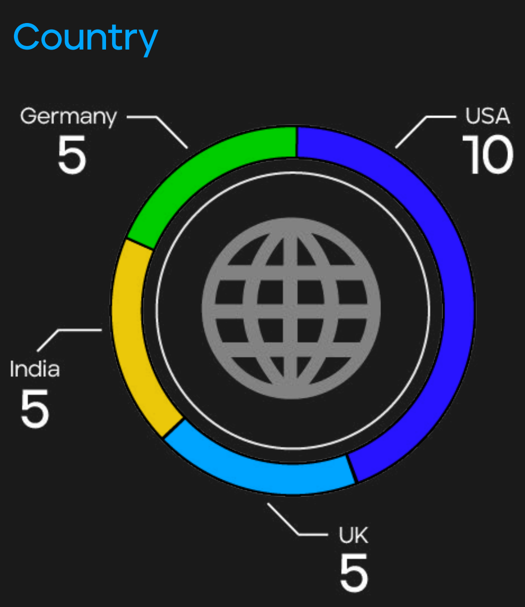


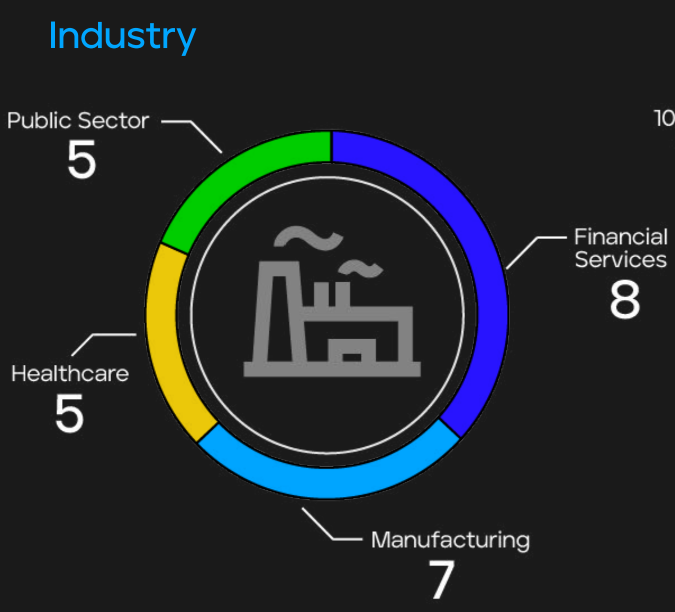
Industry

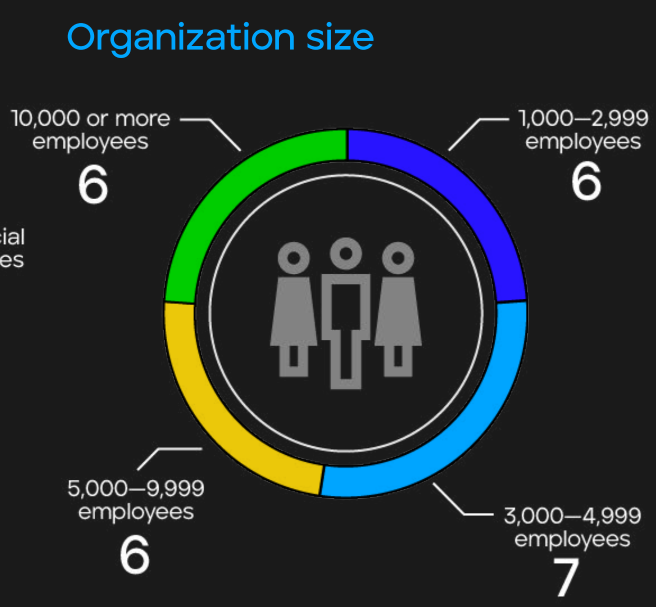


Survey respondents

Qualitative research: We conducted in-depth interviews with 25 CISOs







The invisible hero

CISOs juggle many responsibilities to keep their organizations secure. In the day-to-day, they oversee SOC staff, ensure their employees receive proper training, and report back to other business leaders.

On a larger scale, they manage their organization's cybersecurity program, align to business goals, and build a culture of strong information security.

Clearly, these are monumental tasks. Especially in a field that's impacted by constant innovation of both security pros and malicious actors. Not to mention, organizations continue to transform and grow, requiring CISOs to adapt to stay one step ahead of evolving security needs.

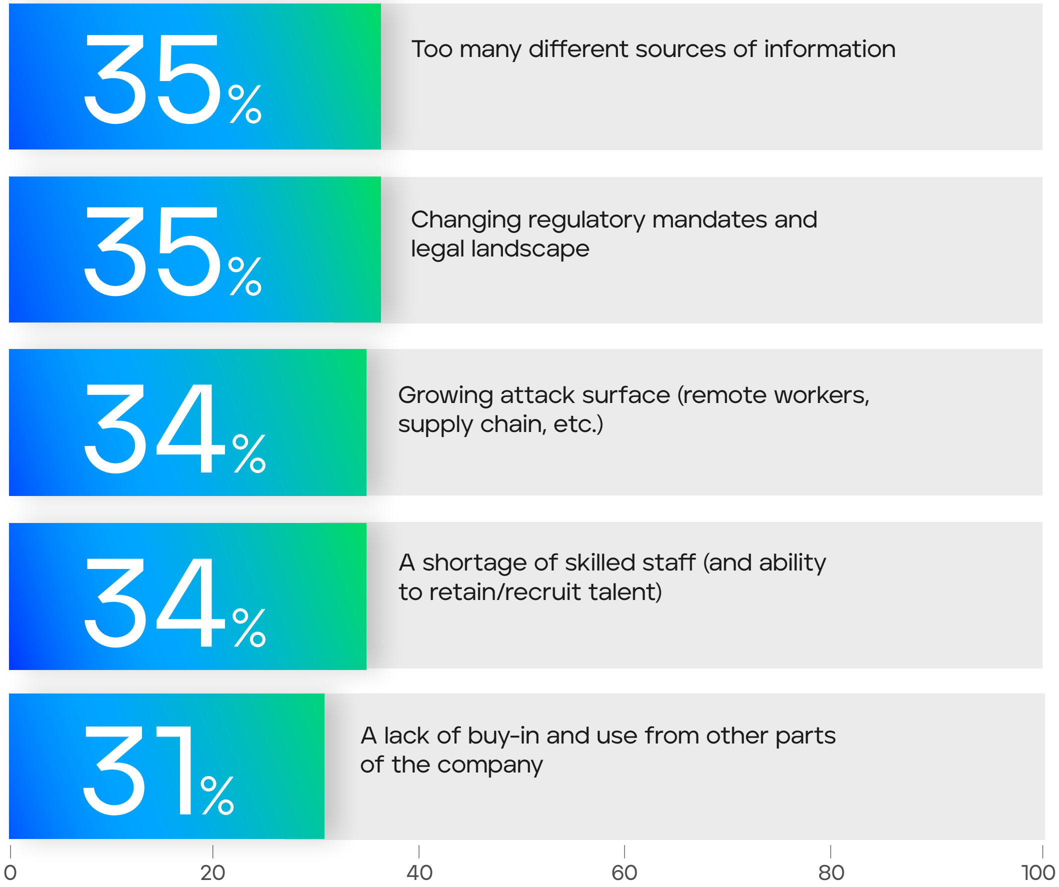
> // The better I do my job, the more I'm a ghost. And if I'm a ghost, you don't see me."
>
> —CISO, Financial Services, USA

Despite working so hard, this is often a thankless role. CISOs are invisible when a hundred things go smoothly, because that's what's expected. Much like being a goalkeeper, you could save nearly every shot in a game. But when one slips past you and your team loses 1-0, you shoulder all the blame.

> // You are a hero and held in high esteem and everything is hunky-dory until it's not. So when there are no cyber incidents, it's a job that's well respected. But your head is on the chopping block the moment there's a problem."
>
> —CISO, Financial Services, UK

The top 5 CISO challenges

In such a complex role, CISOs face many hurdles. According to our survey, here are the 5 biggest CISO challenges.



What do these challenges have in common? All five are made worse when the wrong technology is in place. And it's a sad reality, with over half of organizations (51%) planning to maintain or grow their investment in outdated tools like SIEM.

> // We carry a lot of risk and potential stress on our shoulders. If something does go wrong, a lot of fingers get pointed at our role, even when it's sometimes not our fault."
>
> —CISO, Financial Services, UK

Drowning in security tools

Organizations are doing the best they can with the tools they have. But SOC teams are flooded with alerts. They lack what they need to prioritize what matters most. And they generally don't have the visibility required to respond in a timely manner.

Plus, as organizations hold on to technological debt and continue to add more tools, they end up with a disparate mix and too many products. More than half of all organizations (58%) use more than 20 security solutions. And even with so many tools, only 34% of CISOs say they have what they need for their organizations to be cyber resilient.

Instead of making things easier, this onslaught of inadequate tools adds work for CISOs and SOC teams. They spend valuable time on tedious manual tasks and work late to catch up.

Not only do they spend extra time, but the wrong tools lead to more stress. In their current or past role, 86% of CISOs have managed a major cybersecurity incident. When a breach happens, 72% feel fully or mostly accountable. And they report feeling "worried" and "under pressure" as they resolve the incident.

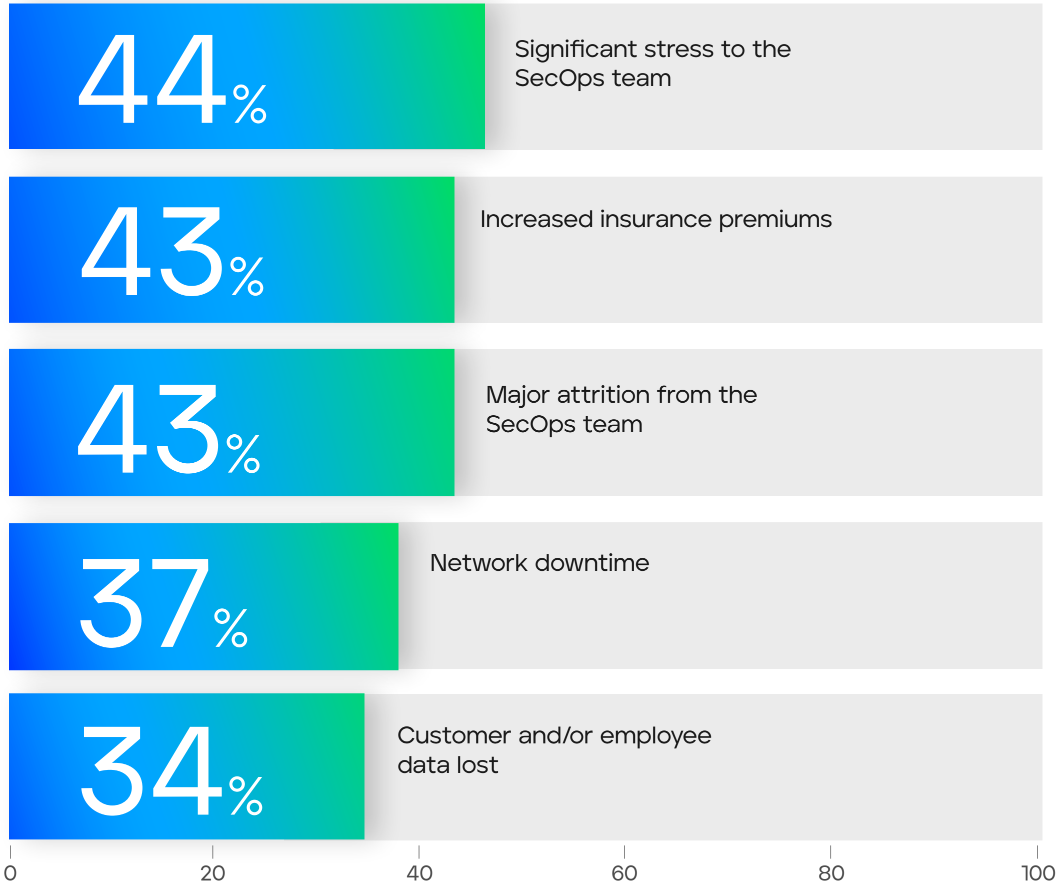
25

The average number of security tools per organization

> Trust is a hard thing to build and it's an easy thing to lose, and so that's what keeps me up at night.
>
> —CISO, Public Sector, USA

Top 5 cyberattack impacts

In addition to how tough a cyberbreach is on a CISO, the impacts can be catastrophic to the rest of the organization. Of those who have experienced a large security incident, they report the following impacts.



How does a major incident feel?

> It is absolute hell, as anybody will tell you, to go through that. It's the pit in the stomach when you start to hear about it. It's the whole roller coaster of maybe this is nothing and then it's something."

—CISO, Healthcare, USA

Empowering the protector

The challenges CISOs face are significant and come with a lot of pressure. But CISOs also reliably show dedication, intelligence, and deep expertise that proves they're up to the task of improving resiliency. In fact, according to survey respondents, their number one motivator is "the changing nature of the challenges."

CISOs flock toward security leadership to protect. They're inspired to take on the role to keep people, data, and other critical assets safe. Not surprisingly, the number one descriptor they identify with is "protector."

This mindset makes for an outstanding CISO. But it's not enough to simply want to overcome the changing nature of security challenges or keep evolving threats at bay. Part of being an effective protector is the willingness to invest in improving security tools and processes.

#1 CISO motivator

The changing nature of challenges

#1 CISO descriptor

Protector

Maximizing your budget’s value

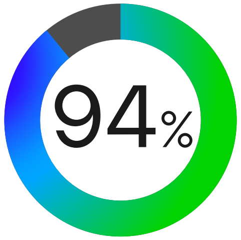
On average, organizations allocate 34% of the IT budget for cybersecurity. Each year, they direct most of their money toward network detection and response ($6.65m) and the least of their money to security operations and analytics ($4.33m).

By allocating ample budget between different areas of security—and ensuring those pieces are connected—technology starts to make jobs easier and lives better.

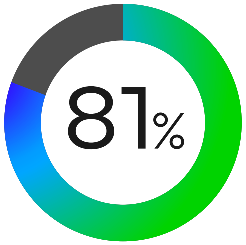
For one, cutting-edge tools can help SOC employees and CISOs automate processes and streamline tasks. According to our research, 94% of CISOs agree that having the right technology in place would save them significant time.

On top of eliminating certain painstaking tasks—allowing them to automatically detect threats, investigate incidents, and respond to attacks—better tools would give SOC staff and CISOs alike the gift of time. In our survey, 81% of security leaders say having the right technology would reduce the number of overtime hours they work.

How would the right technology change CISOs’ lives?

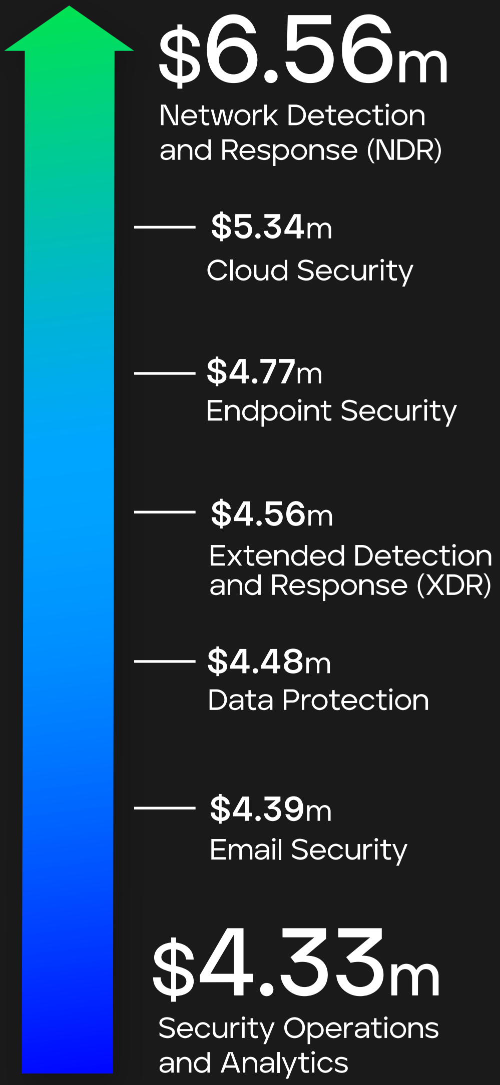


say the right technology would save them significant time



say the right technology would reduce their overtime work

Average budget
(millions of US$ in FY22/23)



$6.56m
Network Detection and Response (NDR)

$5.34m
Cloud Security

$4.77m
Endpoint Security

$4.56m
Extended Detection and Response (XDR)

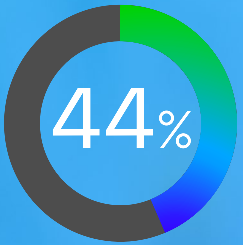
$4.48m
Data Protection

$4.39m
Email Security

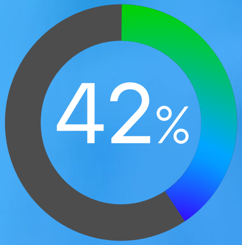
$4.33m
Security Operations and Analytics

Defining the ideal solutions

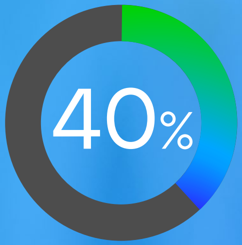
CISOs share the top qualities that would be a game-changer for their security solutions.



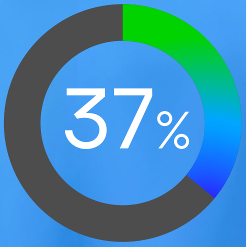
Better visibility



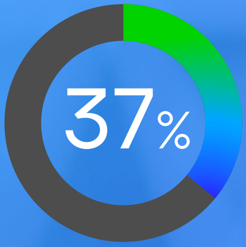
Better prioritization of what matters



Work better together to address multivector attacks



More prescriptive and insightful



Better accuracy

Building the SOC of the future

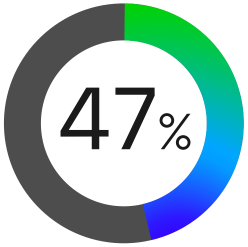
Many of the qualities that CISOs wish their solutions offered—like better visibility, accuracy, and prioritization—are an inherent part of extended detection and response (XDR).

With the right XDR platform, organizations can leave the troubles of the past behind.

Yesterday, CISOs struggled to make sense of all their data with no single source of truth. They grappled to comply with constantly changing regulatory requirements. And they scrapped to defend the business with an inadequate number of staff.

But guess what? Yesterday's over.

Now, you can simplify the cybersecurity experience—building the SOC of the future and taking on today's top challenges through the power of XDR.



already use XDR and expect to maintain or grow it

Rising up in the SecOps revolution with XDR

Your hardworking SecOps team is primed for change and ready to work smarter, not harder. At Trellix, one of our goals is to enable next-level capabilities with the right technology, so your employees can be more efficient and your organization's security approach can be more effective.

The Trellix XDR platform:

Unites disconnected tools, letting you tear down the walls between your solutions and get a complete picture of your security landscape with open APIs and a unified dashboard.

Lowers total cost of ownership, empowering you to consolidate your technologies, correlate data across your products, and maximize the investment in your tools.

Boosts SecOps effectiveness, intensifying your defense against dynamic threats by tapping into groundbreaking AI and ML tools.

Streamlines SecOps efficiencies, allowing you to conquer complexity with defensive playbooks and guided investigations instead of being up to your neck in alerts.

Ready for a revolution? Check out trellix.com to learn how you can take the next step toward your future SOC.

> “The thing I really enjoy about being a CISO is that you are doing a job that protects the organization from a potentially catastrophic event. With great power comes great responsibility and I like knowing that I’m a line of defense for that.”
>
> —CISO, Public Sector, USA

About 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 trellix.com.

Trellix
6000 Headquarters Drive
Plano, TX 75024
www.trellix.com