THE ESSENTIAL CISO PRIMER

Cyber leaders open up about the main issues at play.

CybelAngel

We've reached an irrevocable turning point in this industry.

Cybersecurity's rhythms now pulse with AI turbulence and renewed debates around data trust.

Today's CISOs command not just attention, but influence in the boardroom, especially as organizations brace for sophisticated AI-powered supply chain attacks, rising insider threats, and this April's controversial EU digital identity mandates impacting global operations.

We're living through an AI-fueled trust crisis.

As the lines between cyber offense and defense blur, and as intelligent malware, human machine teams, and coordinated misinformation campaigns redefine risk, we wanted to talk to those on the front line of defense.

We listened extensively to CISOs and senior cyber professionals about navigating complexity once again, for the second edition of this primer. Their insights, both candid and intriguing, paint a picture of the real issues and challenges that CISOs and senior cyber professionals face today.

We know you'll enjoy these insights, and have your own thoughts too.

Happy reading,

Gregory Faitas,
Deputy CEO, CybelAngel

This report is intended to highlight the current challenges the cyber security professionals face.

We would like to thank the cybersecurity professionals who took the time to discuss their valuable experiences and knowledge with us. Their willingness to share crucial information has contributed significantly to our research. Thank you also to the REACT CybelAngel analysts for their help with this research.

A special thank you to the following:

Gerhard Burtscher
Head of Information Security at SEFAR

Olivier Busolini
Group CISO, at Mashreq Bank

Jaïs Pingouroux
CISO and Engineering Manager, CybelAngel

Niamh Vianney Muldoon
CISO, DPO, Board Member

CONTENTS

PILLAR N°1

OPTIMIZATION

CISO CONCERNS AT A GLANCE

What is front and centre for CISOs in 2025?

AI IS STILL TOP OF MIND

Generative AI is driving high-volume, sophisticated phishing, polymorphic malware, and deepfakes that are hyper realistic. Data shows that 80% of CISOs see AI social engineering as a primary threat.

PERSISTENT TALENT GAPS

A cybersecurity talent shortage continues, worsened by a rising demand for AI security and much sought after cloud specialists. Recruitment, just like in last year's eBook, is still patchy, painfully long, and time consuming.

BURNOUT IS GOING NOWHERE

Work stress among CISOs is climbing to record levels, with 94% of CISOs surveyed this year reporting job related stress that is affecting performance and beyond. Data shows that 63% have experienced or observed burnout this year.

TOOL SPRAWL AND INTEGRATION DEBT

Security tool ecosystems remain puzzlingly fragmented and complex, draining resources, creating blind spots, and much more.

COMPLIANCE AND REGULATORY PRESSURE

Regulatory demands are tightening globally, and this is one of the biggest challenges, owing to increased accountability for compliance posture and incident handling.

I. TOOLS

Our strategy is, first, to ensure we are maximizing the use of our existing tools. Often, organizations use only a small fraction of their platform's actual capabilities.

Second, we are adopting a "good enough" strategy. I would rather have a new capability, or replace an old one with adequate coverage, if it integrates with the rest of our security ecosystem. Therefore, prioritizing integration and the ability to cross-correlate over isolated, best-in-class solutions is extremely valuable to me.

Olivier Busolini
Group CISO for Mashreq Bank

Security teams today are drowning in a crowded landscape of tools. On average, organizations juggle over 75 security products from a mix of vendors, creating a patchwork that's tough to manage. In some larger enterprises, the number can be even higher.

This flood of new security tools isn't just a hassle, it is also putting real pressure on organizations and making leadership nervous. CISO data is aligned, with respondents sharing that their teams feel swamped by the sheer volume of security products they have to wrangle every day. A Gigamon survey in late 2024 found that 6 in 10 CISOs listed tool consolidation and optimization as their number one priority for remediating blind spots.

This problem isn't just about complexity headaches; it has a direct impact on an organization's security posture.

What is more, this sluggish environment is killing cyber productivity.

Why?

Well almost half of CISOs, 44% to be exact, in the same report were **unable to detect a data breach in the last year using their existing security tools.**

I. TIPS »

FOCUS ON OPTIMIZATION AND CONSOLIDATION THIS YEAR:

Tool sprawl drains resources, increases risk, and keeps costs climbing. So, ask yourself is consolidation not a trend that you can get behind? It is certainly taking off in certain industries, with 50% of CISOs saying their top priority is reducing the number of security platforms and vendors, aiming for greater control and resilience.

MAXIMIZE ROI AND IMPROVE VISIBILITY:

Platform consolidation delivers real financial impact. Organizations using unified security platforms see up to four times greater ROI than those struggling with fragmented stacks, averaging 101% ROI versus just 28%, according to a 2025 study by IBM and Palo Alto Networks. Streamlining the stack also sharpens visibility: when controls, logs, and alerts flow through fewer interfaces, analysts can spot threats and investigate incidents with less noise and more context. In fact, consolidated environments report 72 days faster threat identification and +84 days faster mitigation compared to those with sprawling, disconnected toolsets. Make sure every tool is simplifying your operations with regular audits.

ADDRESS TALENT AND BUDGET SQUEEZE:

With budgets tightening (reportedly down to 6.4% of overall IT spend for cybersecurity this year!) and hiring remains competitive, it is a shock to know that teams need to do more with less. Leaning into consolidation will only help you to optimize headcount; so your team can specialize in fewer systems and develop deeper expertise. Integration also trims ongoing training costs, fights alert fatigue, and helps CISOs prove the value of every dollar spent to boards and executive teams.

II. DATA

The explosion of security tools has created a secondary crisis: a deluge of data. Security teams are overwhelmed by a tsunami of alerts, with some reports showing that the average SOC receives up to 10,000 alerts every single day.

> Transparency and integrity in breach response are crucial.

Niamh Vianney Muldoon
CISO, DPO, Board Member

CISO data confirms that alert fatigue is a primary driver of analyst burnout and turnover. The sheer volume makes effective triage impossible. A study by the Enterprise Strategy Group found that due to this overload, up to 54% of daily alerts are never investigated, and many of those are simply ignored or suppressed.

This problem directly undermines an organization's resilience. When analysts are forced to chase thousands of low-fidelity alerts, their ability to respond to genuine, high-stakes incidents is critically impaired.

Why is this happening?

Because the security stack is generating data faster than teams can process it. A recent report from Forrester highlighted that 39% of CISOs admit their teams have likely missed or ignored a critical threat in the last year simply because it was buried under a mountain of false positives.

We have conducted a lot of efforts in the last two years to fine-tune our platforms, at least the ones that are the most verbose. Fine-tuning obliges us to really understand what is important versus what is not. This is not a decision we take ourselves; it's a decision we take by speaking with our stakeholders.

This has been fantastic, and makes sure that we have less noise and more actual incidents.

Olivier Busolini
Group CISO for Mashreq Bank

I. TIPS »

PRIORITIZE THREATS, NOT JUST ALERTS:

Agility comes from focusing on what matters most. Shift your team's mindset from clearing an alert queue to neutralizing impactful threats. A SANS Institute study found that teams using a risk-based prioritization model, which factors in asset criticality and attack feasibility, resolve major incidents up to 60% faster than teams working through alerts chronologically.

AUTOMATE TRIAGE AND ENRICHMENT:

Your senior analysts are much too valuable to be copy-pasting IP addresses into lookup tools. Implement automation and SOAR platforms to handle the initial triage and data enrichment for incoming alerts. This frees up your human experts to focus on complex investigations. Data shows that effective automation can reduce manual triage efforts by as much as 80%, giving your team back hundreds of hours per year.

INTEGRATE EXTERNAL THREAT INTELLIGENCE (ETI):

Raw alerts from internal tools lack context. An alert for a strange outbound connection is noise; an alert for that same connection to a known C2 server used by a ransomware group targeting your industry is an actionable signal. A recent Mandiant report noted that security teams with integrated ETI were twice as likely to proactively discover a major incident before it caused widespread damage.

III. EXPOSURES

Find your real crown jewels and protect them.

Gerhard Burtscher
Head of Information Security at SEFAR

You can't be agile if you are misinformed.

For many cyber professionals, the biggest source of risk isn't a known vulnerability, but an unknown asset. The rise of cloud services, IoT, and remote work has created a sprawling and often unmanaged external attack surface. Analysts estimate that this "shadow IT" can account for up to 40% of an organization's total technology environment.

This isn't just a governance headache; it's a CISO's blind spot. Every forgotten cloud storage bucket, abandoned test server, or exposed developer API is a potential foothold for an attacker. It's a risk that CISOs are acutely aware of, with 70% stating in a recent survey by Panorays that they are concerned their teams lack sufficient visibility into the external attack surface.

This lack of visibility has a direct and measurable impact on an organization's resilience. So, what do real consequences look like?

A 2025 report by the Ponemon Institute and IBM revealed that attacks targeting previously unknown or poorly managed assets were the root cause of 21% of all data breaches last year. Again and again you can't defend what you cannot see.

We went from communicating metrics that were a bit of a mix between risk and performance indicators to really having discussions around risks and the appetite for risk.

For example, I never report the raw number of vulnerabilities, as this is a meaningless metric. Instead, I report on our patching performance for the most critical and exposed assets. This approach directly links our cybersecurity risk to the bank's exposure through its externally accessible assets.

Olivier Busolini
Group CISO for Mashreq Bank

I. TIPS »

ADOPT AN EXTERNAL-IN MINDSET:

Don't just rely on what your internal scanners tell you. To be truly resilient, you must see your organization the way an attacker does—from the outside. Implementing an External Attack Surface Management (EASM) program is no longer optional. Organizations with a mature EASM program discover critical exposures 75% faster than those relying solely on periodic internal scanning, according to ESG research.

MAKE DISCOVERY CONTINUOUS, NOT PERIODIC:

Attackers are using automated tools that scan the internet constantly. A quarterly vulnerability scan is no match for this. Data shows that a critical cloud misconfiguration can be discovered and exploited by automated tools in under 10 minutes. Your discovery process must be just as relentless. Agility requires a real-time, continuously updated inventory of all your internet-facing assets.

TIE EXPOSURES DIRECTLY TO BUSINESS RISK:

Finding an exposed port is a technical finding. Finding an exposed port on a server that processes customer payment data is a business risk. CISOs must be able to translate their attack surface data into a language the board understands. In fact, according to Gartner, by 2026, 50% of CISOs will be required to formally report on the business risk associated with their cyber-physical systems and external exposures. Get ahead of this trend by prioritizing remediation based on business impact, not just CVSS scores.

PILLAR
N°2

AI ADOPTION

> AI is no new game. AI is just another player.

Gerhard Burtscher,
Head of Information Security at SEFAR

The rise of AI represents the most significant dual-use technology CISOs have faced in a generation. It is simultaneously a formidable threat multiplier and an unprecedented opportunity for defense, automation, and innovation.

This paradox has placed AI at the absolute top of the CISO agenda, after all Generative AI tools are a dime a dozen today.

The numbers support this as over 70% of enterprises now use generative AI in at least one business function, up sharply from 33% in 2023, and analysts estimate 78% of organizations overall have integrated AI technology into core operations. CISOs themselves are taking a pragmatic approach to AI in security. 87% of those surveyed by Proofpoint this year are adopting or evaluating AI-based tools to address advanced threats and reduce the risks posed by human error.

But it is not all smooth sailing.

72% of CISOs are worried that gen AI solutions could result in a significant breach, as adversarial AI data poisoning techniques, like ConfusedPilot, that target RAF based AI systems, become de rigueur. A malicious actor might want their phishing emails to systematically bypass the aforementioned filter.

> Right now, one of the biggest concerns is shadow AI, when cloud apps or third parties turn on AI without proper oversight.

Niamh Vianney Muldoon
CISO, DPO, Board Member

“The transformation of the bank is material, thanks to AI. Our job for the last two years has been to make sure that we are part of this bullet train and that we are really addressing or removing issues left and right, while at the same time maintaining guardrails specifically related to data leakage and privacy. Finding this balance has been a very important objective, and I think that we have achieved that significantly by partnering with the business, with the data teams and, later, the AI team.”

Olivier Busolini
Group CISO, at Mashreq Bank

“Results from AI must be proofed to ensure they are true and good enough to use for business purposes. In my opinion, this is the greater risk: using incorrect information for business purposes and making wrong decisions that cause damage.”

Gerhard Burtscher
Head of Information Security at SEFAR

“At CybelAngel, we believe that the future of SOC teams lies in Agentic AI processing Level 1 and 2 incidents, leveraging SI human expertise where it is really needed for the most complex and delicate matters. It is with this in mind that we have developed our roadmap for 2026, to empower our customers with self-served, enriched incidents and contextualization, directly available through MCP servers.”

Jaïs Pingouroux
CISO and Engineering Operations Manager at CybelAngel

The shift is also a structural change in how security itself is run as improved posture data emerges.

Agentic AI is the next big subject for cyber professionals. According to Gartner and Forrester, Agentic AI represents a significant evolution in artificial intelligence technology (it is a top AI Gartner trend for 2025).

Unlike traditional AI, agentic AI systems act autonomously, making decisions, adapting dynamically to threats, and executing complex security workflows with minimal human input. So, what will this additional layer of complexity mean for cyber teams? For one on the team front, it will mean great efficiency, less cost, less human error. It also means sharper threat detection, reduced alert fatigue, and more effective incident response.

With data pointing to its "work in progress" status, tech leaders are jumping on board. In a 2025 survey by Georgian and NewtonX, 45% of technical leaders reported currently using agentic AI, with an additional 19% planning implementations by the end of the year.

We are now in an interesting context where we not only have AI but are also starting to see developments in quantum computing. The combination of quantum and AI could be explosive.

We continue to look at emerging risks, ensuring we are not just surfing today's AI wave but, like any good surfer, are already looking for the next one. The potential merger of supercomputing and AI is an interesting emerging risk we see on the horizon. Looking at the wave behind that, quantum computing also brings fascinating developments like homomorphic encryption—the ability to perform calculations on encrypted data without having to decrypt it first.

While our focus is on AI, we are mindful that quantum is next, and it is opening the door to many new possibilities.

Olivier Busolini
Group CISO, at Mashreq Bank

I. TIPS »

LEAD AGENTIC AI GOVERNANCE:

Your role now includes setting governance frameworks specifically for autonomous AI systems. Gartner forecasts agentic AI will automate 15% of routine decision-making by 2028, making early policy creation and oversight crucial to avoid risks.

TELL YOUR TEAM ABOUT AGENTIC AI NUANCES:

Nearly half (45%) of technical leaders report currently using agentic AI, with another 19% planning implementations this year. Ensure your security team grasps its autonomy and limits so they can identify threats accurately and know when to escalate.

ADOPT AN EXTERNAL-IN MINDSET:

Don't rely solely on your internal scanners. Organizations with mature External Attack Surface Management programs identify critical exposures 75% faster than those only using periodic internal scans.

MAKE DISCOVERY CONTINUOUS, NOT PERIODIC:

Automated attackers scan constantly. A quarterly vulnerability scan won't keep up. Data shows critical cloud misconfigurations can be exploited in under 10 minutes. Your discovery process must be consistent.

TIE EXPOSURES TO BUSINESS RISK:

A technical finding isn't a business risk until it impacts your operations. By 2026, 50% of CISOs will be required to report formally on business risks linked to cyber-physical systems and external exposures. Prioritize remediation by business impact, not just CVSS scores.

SHIFT FROM REACTIVE TO STRATEGIC SECURITY:

Agentic AI can reduce the time from threat detection to remediation from weeks to minutes by autonomously managing monitoring and response. Integrate AI agents to free your team for complex threat analysis and improve efficiency.

PILLAR N°3

COMMUNICATING VALUE

I. HITTING THE RIGHT NOTE

How do you translate complex cyber risk into a language the board understands and acts upon? What metrics show your real value? Where do you start when it comes to threading complex subjects like tool consolidation, budgets, and compliance into your cyber board brief?

> We take the opposite approach. I like to define risk as the point where danger meets vulnerability. We don't analyse the danger (the cyber attack) but rather the vulnerability (the business process). We evaluate business processes according to their criticality.

Gerhard Burtscher,
Head of Information Security at SEFAR

These are the questions every CISO faces.

You need to stay nimble to frame cybersecurity as a core business priority, and keep the messaging clear that the tech is not the only thing protected, but also brand reputation, revenue, and operational resilience.

> Communicating risk is a major challenge for CISOs. It's important to translate complex technical issues into clear business risks for boards and executives. Many of them aren't technically minded, but they need to understand the business impact and consequences if a risk materializes. This ultimately includes the financial costs—both direct and indirect, such as the loss of trust.

Niamh Vianney Muldoon
CISO, DPO, Board Member

The days of overwhelming the board with dashboards full of vulnerability counts and blocked phishing attempts are over. A 2025 Deloitte report highlights that 78% of board members feel their cybersecurity reports are overly technical and fail to connect threats to tangible business outcomes. CISOs need to convert the complex into a simple, clean business context.

This year cyber teams are shuffling from noting activity metrics to outcome-driven metrics in their reporting. Instead of reporting on what the security team is doing, the focus must be on what the business is achieving. It's the difference between saying "We blocked 500,000 threats" and "We reduced the financial risk exposure of our crown jewel assets by 40% this H1."

According to the Evanta 2025 CISO Priorities Survey, cyber resilience, which relies heavily on communication across departments, is the top CISO priority. Yet only 44% of CISOs have direct communication channels to their CEOs, per SANS Institute, limiting effective advocacy. Boards consider poor communication among top factors in underwhelming security program support.

It's a very long journey to move from a traditional way of looking at control gaps and security KPIs to looking at risks. It's a very long journey to speak about actual risk and not forget that risk is a mix of articulating with your business what processes your organization really depends on, and what underlying IT processes and assets support those critical business processes.

Only when you are able to articulate the first part (the likelihood of an event) with the actual business impact can you speak about risks. But people are still focusing a lot on the first part and not considering the second part of the risk to the extent that it should be. And so they are talking more about control gaps or technical weaknesses, rather than risks.

Risk means taking into consideration what is at stake for the organization, not what is at stake for security.

Olivier Busolini
Group CISO for Mashreq Bank

I. TIPS »

BUILD TRUST DURING YOUR BRIEFS:

Your briefings should be tailored for each audience, whether it's the CEO, CFO, or the entire board. For the CEO, you'll need to show how cybersecurity bolsters business resilience and brand reputation. For the CFO, you'd focus on financial risks and ROI. Having data from executive dashboard tools will help you to nail precise questions.

REPORT ON OUTCOME-DRIVEN METRICS (ODMS):

Use metrics that connect security efforts to business impact. In 2025 these look like Time to remediate critical AI vulnerabilities, Third-party AI supply chain risk, Ransomware recovery time objective (RTO), and Endpoint protection against AI-generated malware.

SET UP YOUR REVIEW CYCLES OFTEN:

Don't wait for the next big board meeting. A disciplined, ongoing review process for key metrics keeps your team focused and prevents any surprises. If you share updates on incident response times, vulnerability mitigation, and threat detection effectiveness build confidence. By 2026, Gartner says that half of CISOs will be required to report on the business risks associated with cyber-physical systems and external exposures, so getting ahead of this trend will set you apart

---

COMMUNICATE SIMPLY:

This is as simple as talking your board's language. It is your job as a leader to translate complex cyber issues into financial and operational impacts for the benefit of your team. When your security metrics tell a story about what matters, like potential revenue loss or regulatory penalties, you gain trust and influence.

II. Navigating compliance

The January 2025 enforcement of The Digital Operational Resilience Act (DORA) is reshaping how financial institutions approach digital resilience in Europe. It is the backbone of a unified EU approach to managing ICT-related risks.

From the landmark EU AI Act to California's evolving privacy regulations, new legal frameworks are emerging worldwide, begging the question how compliant is your organization?

This isn't merely a bureaucratic hurdle; adherence is critical to avoiding substantial fines (Forrester predicts that breach-related class-action costs will surpass regulatory fines by 50% in the coming year), reputational damage, and legal liabilities.

Diverted resources are another issue in the struggle with regulatory adherence.

In nervous conditions for markets, achieving and maintaining compliance amid new changes and challenges lends itself to credibility. As large companies embrace a skittish global market, compliance is a competitive differentiator. The simple act of using a generative AI tool could inadvertently trigger serious compliance issues across multiple jurisdictions like GDPR, CCPA, or HIPAA if data is transmitted improperly.

So, how are cyber leaders navigating this immense pressure?

> I don't fear that an employee might deliberately disregard compliance. Instead I fear that an employee does not follow rules because they have no idea that an action is not compliant. To prevent this, we need a sufficient level of awareness.

Gerhard Burtscher,
Head of Information Security at SEFAR

Compliance alone won't stop breaches. It's vital to balance compliance efforts with active risk management, marrying compliance and risk programs.

From a European perspective, there's a big push on digital assets and cryptocurrency regulation. In Ireland alone, 30 companies are seeking MiCAR approval to trade in crypto assets. This will increase execution threats if organizations don't have proper business processes like segregation of duties and technical controls like multi-factor authentication in place.

Niamh Vianney Muldoon
CISO, DPO, Board Member

I. TIPS »

BECOME A GLOBAL REGULATORY STRATEGIST:

You must look beyond your local jurisdiction and develop a global compliance strategy. According to Gartner research, 75% of the world's population will have its personal data covered by privacy regulations by the end of 2025. This requires continuously monitoring the evolving landscape of international laws to keep your organization ahead of new requirements.

TRANSLATE COMPLIANCE INTO RISK REDUCTION:

Your board and executive team need to understand that compliance does not automatically equal security. Frame the conversation around ROI by highlighting that the cost of non-compliance is nearly three times higher than the cost of meeting regulations, according to a study by the Ponemon Institute. This proves that investments in frameworks like NIST CSF 2.0 deliver a tangible reduction in financial and cyber risk.

INSULATE YOURSELF AND THE BUSINESS FROM LIABILITY:

With CISO liability a major concern, meticulous documentation is your best defense. This is especially critical since regulators like the U.S. Securities and Exchange Commission (SEC) now have rules mandating detailed public disclosures on cybersecurity governance and risk management, increasing scrutiny on leadership decisions. Your documentation creates a defensible position for both you and the organization.

CHAMPION A CULTURE OF DATA GOVERNANCE:

The use of generative AI requires a renewed focus on data governance. Emphasize to leadership that unsecured AI usage is a primary source of risk. As highlighted in a recent Zscaler threat report, enterprise traffic to AI applications has increased by nearly 600% over the last year, dramatically expanding the threat surface and making strong internal data policies more critical than ever.

WRAPPING UP

We've come full circle in this primer.

The foundational assumptions of cybersecurity are being rewritten. The proliferation of AI is introducing a level of ambiguity that renders static, perimeter-based security an obsolete model.

1. **Design for adaptation** because brittle, monolithic defenses fail unpredictably. A modern security posture is composable and built to respond to new signals in real time. The objective is not just to block threats, but to create a system that learns and reconfigures itself intelligently.

2. **Treat trust as a protocol** as human and machine interactions become indistinguishable. Trust needs to evolve from an assumption to a verifiable process. This means engineering explicit checks for identity and data integrity into every layer of your infrastructure, reducing ambiguity and creating reliable signals.

3. **Integrate security as a business primitive** because CISO's function is moving from a gatekeeper to an enabler of programmatic growth. When security is integrated as a core component of the business—akin to an internal API—it stops being a bottleneck and becomes an accelerator for product development and market expansion.

Resilience is not an outcome, but an architectural principle. It is achieved through intentional design choices that favor flexibility, explicit verification, and deep integration with the business. The goal is a security posture that provides the stable foundation required to accelerate what you build next.

CISO RESOURCES

1. CISA's Ransomware Webpage
2. FBI Ransomware Resources
3. #StopRansomware: Interlock Ransomware Advisory (2025)
4. #StopRansomware: RansomHub Ransomware (2024)
5. CISA's Cyber Safety and Resilience Toolkit
6. U.S. Secret Service Ransomware Advisory
7. U.S. Department of Health and Human Services (HHS) Ransomware Guidance
8. Australian Cyber Security Centre (ACSC) Ransomware Guidance
9. UK National Cyber Security Centre (NCSC) Ransomware Guidance
10. Multi-State Information Sharing and Analysis Center (MS-ISAC) Ransomware Guide
11. FINCEN's Advisory on Ransomware and the Use of Virtual Currency (2024 update)
12. NIST Cybersecurity Framework (CSF) 2.0 (2024)
13. Draft NIST SP 1331: Quick-Start Guide for Using CSF 2.0 to Improve Management of Emerging Cybersecurity Risks (2025)
14. The No More Ransom Project
15. ENISA Threat Landscape 2024
16. ENISA Threat Landscape for Ransomware Attacks
17. Institute for Security and Technology (IST) - Ransomware Task Force Report
18. Europol's European Cybercrime Centre (EC3) Public Awareness Materials
19. Interpol's Global Cybercrime Programme Resources
20. Ransomware Actor Profiling

CybelAngel

The external threat intelligence platform that secures your business

Secure your digital activities with CybelAngel, the only comprehensive threat Intelligence provider.

TRY CYBELANGEL