Stay connected. Stay safe.

Skyleaf Annual Report 2024

CYBERWOLF
your digital bodyguard

spotit
YOUR SECURITY & NETWORK LAYER

Connecting you.

The first annual report from Skyleaf: a retrospective full of confidence, a forward look filled with ambition.

Since 2014, we have been working with passion and ambition on our mission: to connect people, businesses, and machines — always with a strong focus on security. At spotit, our goal has never been to become the biggest in cybersecurity & networking, but to be the best. Meanwhile, our offering has expanded with Cyberwolf, a kind of 24/7 digital bodyguard for private life. Both companies are part of the Skyleaf holding.

In both companies, we work with top talents, innovative technologies, and services that perfectly match the needs of our clients. Each of them are businesses and organizations that understand how essential it is to invest in high-quality solutions for cybersecurity and networking. We are fully committed to sustainable partnerships. We don't see ourselves as traditional suppliers but rather as a true extension of your company or IT department — someone you can trust 200%.

In this very first Skyleaf annual report, we look back at 2024. We offer an overview of our highlights, consolidate fascinating figures, zoom in on our renewed Security Incident Response offering, and share tips to boost your cybersecurity.

Thank you for your trust. We look forward to writing the next chapters of our story together — whether that's with spotit or with Cyberwolf. In a world where connectivity and security are becoming increasingly important, we look to the future with optimism.

Steven Vynckier en Frederik Rasschaert,
Founders of spotit and Cyberwolf

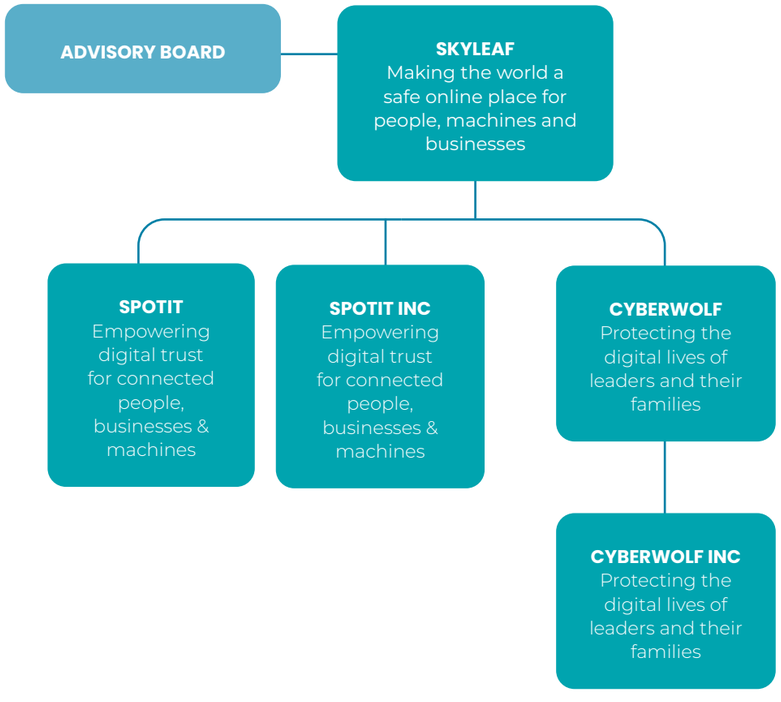
Protecting you.

Who we are

Who is **Skyleaf**?

Our company operates with a holding structure, which means there is a parent company (holding) that oversees several entities. The holding is called Skyleaf, with spotit and Cyberwolf as its entities.

Skyleaf has a clear and important mission: to make the world a safe online place for people, machines, and businesses. In today's interconnected world — where digital threats are constantly evolving — Skyleaf strives to create a secure environment for both individuals and organizations.



Who is **Cyberwolf**?

Cyberwolf is a 24/7 digital bodyguard for the private lives of VIPs—ranging from C-suite executives and board members to ministers, diplomats, and high-net-worth families across the globe. Much like spotit does for businesses, we protect devices, data, email, and accounts, monitor threats, track dark web activity, and intervene during incidents. Our approach is so effective that one of the largest American banks now introduces us to their most affluent families. We're only getting started!

Who is **spotit**?

Our mission
We provide you with peace of mind when it comes to everything related to security and connectivity.
As a strategic partner, we focus on vision, expertise, and trust.

Our promise
We make the difference with a high-level, long-term approach to security and networking. Your security and network are essential parts of your business strategy. That's why we start from an action plan with clear goals. In addition to standard solutions (such as switches, routers, firewalls, and antivirus software), we integrate high-tech expertise, 24/7 managed services, a project-based approach, and crystal-clear reporting.

Spotit at a glance

- Builds and manages cybersecurity and network strategies
- Provides services in 80 countries across 5 continents
- Has offices in Merelbeke-Melle, Herk-de-Stad, and New York
- The group (spotit and Cyberwolf) achieved a turnover of €30 million in 2024 and employs 135 people
- Focuses on companies with 150+ employees
- Is active in all sectors, with leading references in utilities, industry, logistics, pharmatech, and life sciences
- Founders Steven and Frederik still hold 100% ownership

Our values

Trust

Trust is essential — especially in cybersecurity. We handle sensitive data with the utmost care, fully aware that any breach can have serious consequences.

Our belief in confidentiality, integrity, reliability, and honesty is also reflected in our actions: we deliver what we promise, learn from mistakes, and take feedback to heart.

Human to Human

At spotit, we build real connections. We believe that people don't just buy products or solutions — they seek connection. That's why we put colleagues, clients, and partners at the center of every interaction. We tackle challenges together, with open communication and mutual respect. Every day, we work to make our company a better version of itself — through communication and respect as fundamental values.

Excel

To keep our customers happy, we aim to excel. We strive for top performance and never settle for mediocrity. Together, we raise each other to a higher level and continuously challenge ourselves to improve.

Because excellence is not just a result — it's a mindset.

Entrepreneurship

Everyone at spotit has an entrepreneurial spirit. Our team members are given freedom and take responsibility. They act quickly when facing challenges, take initiative, and work together on solutions — even outside their comfort zone. Together, they go the extra mile — and our clients feel that difference.

The 2024 highlights

We celebrated our 10th anniversary

10

In 2024, we proudly marked our 10-year milestone. We gained significant press attention and, of course, celebrated with our team. On June 8, employees and partners gathered at the idyllic Hottentothoeve in Bonheiden. The evening had a “Back to the Future” theme — reflected in the invitations, poster, decorations, drinks, and gifts. Dancing went on late into the night.

Proud of our NPS score: 50+

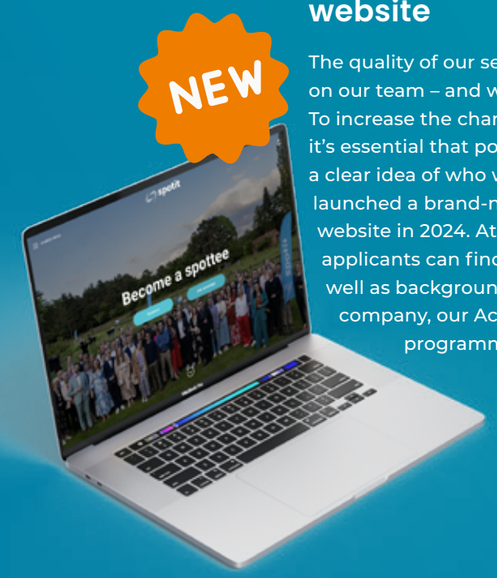
50+

Would you recommend spotit to a colleague or friend? That’s the central question we ask our clients each year through an extensive Net Promoter Score (NPS) survey conducted by an independent firm. It provides us with deeper insights into how our services are perceived and where we can improve. In 2024, we achieved an impressive score of 51. Our clients specifically mentioned our expertise, customer focus, and reliability as key strengths.

x3

Cyberwolf continued its discreet growth in 2024, tripling the number of members.

New talent recruitment website



The quality of our services depends entirely on our team – and we’re well aware of that. To increase the chances of a perfect match, it’s essential that potential candidates get a clear idea of who we are. That’s why we launched a brand-new talent recruitment website in 2024. At jobs.spotit.be, potential applicants can find current vacancies as well as background information about our company, our Academy, and our wellbeing programme.

200.000

Over the past 10 years, we’ve supported numerous charitable initiatives. In 2024, we donated €10,000 to the Suicide Prevention Hotline. Giving back to the community remains a core value.

10 new top talents

In 2024, spotit welcomed 10 new colleagues — each one enhancing our ability to serve clients better, from presales to invoicing. These targeted hires reflect our ongoing investment in excellent and personalized service at every touchpoint.

“Lifeline in case of a cyberattack”

HOTLINE
+32 (0)9 322 04 35

In 2024, we expanded the services of our Cyber Security Incident Response Team. A hack, breach, malware infection, or other cyber threat? Our experts guide you in making your organization operational again as quickly as possible, with minimal impact.

WE RENEWED THE CYBER SECURITY INCIDENT RESPONSE TEAM OFFERING

Today, more than 1 in 8 Flemish companies is affected by a cyber incident. A survey shows that 39 percent of Belgian companies expect to fall victim to a cyberattack in the coming year. Investing in CSIRT is no longer a “nice to have” but an absolute “must have.”

A cybersecurity incident can happen at any moment. Whether it’s a cybercriminal demanding bitcoins via a ransomware attack or incidents with (inter)national impact, our emergency service guarantees a rapid response to limit the damage as much as possible.

Our hotline is available 24/7. You will reach a spotit incident responder who immediately evaluates the situation and maps out the impact. This allows them to quickly advise concrete actionable items to anticipate and prevent further damage.

At the same time, a multidisciplinary team is formed with stakeholders from your company and from spotit.

The team works to contain the incident, remove the hacker from the network, and during the recovery phase, safely restart the environment so you can refocus on business continuity.

Proactive services
With us, it doesn’t stop at reactive assistance after an incident. We also offer proactive support: we monitor your network and intervene at the first signs of suspicious activity. The sooner we can act, the greater the chance of success.

That’s why good preparation is crucial. With our retainer service, our experts are permanently on standby, fully familiar with your IT environment, and can intervene immediately and effectively when necessary.

During onboarding, all necessary information about processes, the environment, roles, and responsibilities is collected. This is followed by a “Breach Readiness Assessment.” You get a clear view of your organization’s ability to identify, investigate, and respond to cybersecurity incidents. We then install a “honeypot warning system” that detects potentially malicious activity early, allowing for quick response to threats.

This service also ensures that all relevant data is kept up to date for all involved experts. A dedicated service manager will regularly plan update meetings, share data, and “lessons learned” with you.

6 reasons why CSIRT is a must

1. **Immediate response:** a cyberattack is like a medical emergency for your organization. CSIRT provides — just like doctors — immediate expertise when you are most vulnerable. CSIRT teams are trained to respond quickly and efficiently, limiting the impact of the attack and allowing normal business operations to resume as soon as possible.

2. **Expertise and specialization:** CSIRTs are the specialized “doctors” in the world of cybersecurity. They possess the expertise needed to diagnose and treat the specific threats your company faces. The team uses advanced tools and techniques to identify the source of the attack, assess the damage, and implement the most effective recovery strategy.

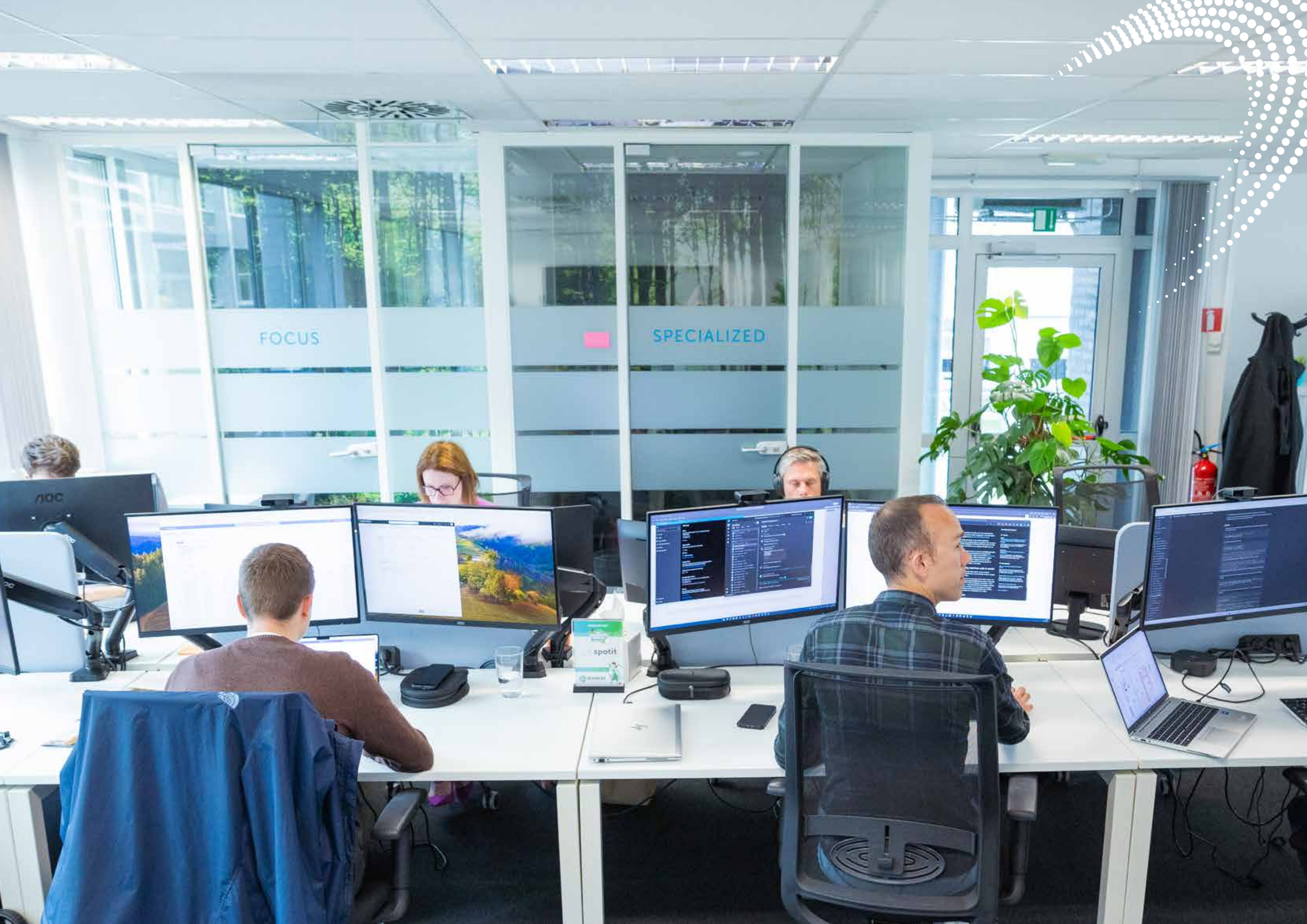
3. **Cost savings:** although it may seem paradoxical, engaging a CSIRT can lead to significant cost savings. Incidents like data breaches and system intrusions can carry enormous financial burdens. A CSIRT significantly reduces the risks and associated costs.

4. **Reactive and proactive:** a CSIRT not only works reactively; it also performs regular checks and updates, helping prevent many attacks. That proactive approach can result in substantial cost savings and safeguard your company’s continuity.

5. **Compliance:** regulations around data and privacy are becoming increasingly strict. A CSIRT ensures your organization complies with relevant laws and standards, which not only avoids fines but also strengthens trust among clients and partners.

6. **Peace of mind:** knowing that an expert team is ready to intervene provides peace of mind. Knowing that your cybersecurity is in the hands of professionals allows you and your employees to focus on your company’s core activities.

FAQ CSIRT


FOCUS
SPECIALIZED
spotit

CASE

Ransomware attack at Santens

Santens is a technical wholesaler in construction hardware and tools, focused on skilled professionals such as carpenters, contractors, technical services, and public administrations. The company, headquartered in Merelbeke-Melle, fell victim to a ransomware attack that rendered its **systems unavailable for several days.** They called upon the CSIRT service of spotit.
The evening before a long weekend, Santens was contacted by the federal police, who reported that account details of Santens were being offered for sale on the dark web. This news marked the beginning of a cyberattack nightmare.

Santens immediately set up a crisis cell with internal staff and external professionals to assess the impact on daily operations. **The management team made quick and decisive decisions.**

Spotit immediately evaluated the situation and impact after the attack. The CSIRT team isolated the infected systems and was able to prevent the ransomware from spreading further. Spotit provided careful guidance and in-depth advice for restarting the systems and implementing additional cybersecurity measures.

Thanks to the good backup systems — which were not affected — Santens succeeded in limiting the damage and was able to restart operations within a week. Santens subscribed to the Managed Detection & Response service, with CSIRT included. Spotit now actively monitors the IT environment for anomalies. If an incident does occur, Santens can count on spotit professionals to intervene quickly.

Before the attack, a cyberattack seemed like something for large companies. After facing an attack and talking to other companies, Santens now realizes that many organizations are affected. Cybersecurity awareness is now high on the agenda. Santens is fully committed to active and ongoing awareness among its employees, especially as it continues to invest in digitization. Digitization and cybersecurity go hand in hand.

"The cyber attack inflicted substantial financial losses on Santens. We faced costs exceeding several hundred thousand euros to get back up-and-running and the lost income easily amounts to €2,000,000. This is a very severe impact for a company like Santens."

Bram Vande Walle, CEO Santens

10 TIPS

for more peace of mind in cybersecurity & networking

Ensure a strong foundation in security
Start with a thorough security audit of your IT environment. Identify vulnerabilities and address them immediately.
01

Implement multi-factor authentication (MFA)
Add an extra layer of security by using MFA for access to critical systems and applications.
06

Implement a zero trust strategy
Trust no one inside or outside your network without verification. Limit access to data and systems only to those who truly need it.
02

Use a reliable firewall and next-gen security solutions
Protect your network with advanced firewalls and intrusion detection/prevention systems to block unwanted access.
07

Invest in end-to-end encryption
Protect sensitive data both in transit and at rest with strong encryption protocols.
03

Conduct regular penetration tests
Simulate cyberattacks to evaluate how well your systems can withstand threats, and improve where necessary.
08

Perform regular updates and patch management
Ensure that all your software, hardware, and operating systems are up-to-date with the latest security patches.
04

Monitor your network 24/7
Use a Security Operations Center (SOC) or automated tools to detect and stop suspicious activities and attacks in real-time.
09

Awareness and training for employees
Employees remain the weakest link in cybersecurity. Provide regular training on phishing, social engineering, and safe online behavior.
05

Create an incident response plan
Be prepared for the worst. Develop a detailed plan that outlines how you will respond quickly and efficiently to a security incident.
10

More info? Contact us!

“Our drive is cristal-clear: we want to be the best”

On June 2, 2024, spotit turned 10 years old. A decade is a long time—especially in a fast-evolving field like cybersecurity. Founders Steven Vynckier and Frederik Rasschaert, who still lead the company today, took a moment to reflect on the journey so far and share their ambitious plans for the future.

How and where did it all start for you?
Steven: “We met while working at an IT company. After a while, Frederik joined my team, and we started working closely together. We clicked and decided to start our own story. We both felt that many companies offering network and security solutions were making quality compromises. So from the start, our focus was clear: deliver top-quality solutions with highly trained professionals and become the go-to reference for connectivity and security.”
Frederik: “Starting our own company was a big step, but entrepreneurship runs in our veins. I’ve always been passionate about technology, got interested in IT through my father, led a youth organization for years, and started freelancing at 18.”

“Thanks to our approach, clients don’t see us as just a supplier, but as a true partner and companion on the journey.”

Steven: “Entrepreneurship was instilled in me from a young age. My father owned a furniture business and my mother ran the store. They gave me lots of freedom and autonomy. I was in the scouts and also competed in athletics at a fairly high level. That reflects who we are.”

What was it like in the beginning?
Steven: “We didn’t want to be just another—excuse the term—box mover selling hardware, software, and licenses. From day one, we chose to be a managed services company. Every engagement starts with an assessment of the current situation, followed by improvements, a clear vision, implementation, and operational management.”
Frederik: “We didn’t have to start from scratch since we already had a strong network. We were fortunate that some of our contacts truly believed in us and supported us from the start, just like the technology partners we worked with.”
Steven: “To fully unburden our clients, we immediately launched a Network Operations Center (NOC). We landed our first NOC client quite quickly—a major milestone. Shortly afterward, we had the opportunity to work for a large Flemish utility company. That was a huge achievement for such a small company and proved we had the right skills.”

Do you have any fun anecdotes from those early years?
Frederik: “When we signed our first NOC contract, we didn’t have a data center, and the cloud wasn’t a thing yet. We started with a few PCs in my garage. What we did was safe and professional, but the equipment was limited. As soon as we could afford it, we invested in a data center in Oostkamp, which we still use today. We later added one in Merelbeke.”
Steven: “Fun fact: in the first four years, we moved offices six times. We started in a business center in Waregem and then moved to Merelbeke, where we’ve changed locations several times and gradually expanded.”

Not everything must have gone smoothly?
Frederik: “That first big project for the utility company was challenging—we were just 18 people at the time. Their CIO really stuck his neck out for us because he believed in us. Three years later, we were called in by the board and told they were very satisfied. That was the best compliment we could have received. We helped them evolve to a stable environment with hardly any incidents, a huge change from their past. They are still a very satisfied client today! Another challenge was how to bring our security operations offering to market. We initially tried reselling software with consultancy on top, but the market wasn’t ready. Budgets were too high, and it wasn’t a top priority yet. We tested other models until six years ago when we invested in our SOC. A Security Operations Center detects anomalies in user and machine behavior, identifies hackers, and uncovers security gaps. We hired the right people for it, and now that offering is fully mature.”
Steven: “More recently, wage indexations posed a challenge. Salaries are our biggest cost, and it’s hard to absorb those increases during tough economic times. We’re a healthy, profitable company, but we have to choose our investments wisely. We tried to launch in the U.S., but had to scale back. We’re still exploring the market, but at a slower pace. American companies aren’t exactly waiting for a Belgian player, we learned.”

What makes spotit so special and unique today, in your opinion?
Steven: “The reason we founded spotit and our strategy have not changed. We continue to focus on networking and security, with quality as the cornerstone and always with a long-term vision. And it works, because our customers say we deliver what we promise. They are true ambassadors for us.”
Frederik: “We truly create value for our customers—through our technology but also by thinking along with businesses. And we also make a difference by striving for real partnerships with our clients. In any relationship, there are moments when things don’t go as planned; it’s about handling those well. Thanks to this approach, clients don’t see us as ‘just a supplier’ but as a real partner and companion on their journey.”

What drives you the most?
Frederik: “I’ve always enjoyed creating value through technology. It’s very rewarding when a customer achieves results thanks to us—and appreciates that.”
Steven: “I get energy from launching and growing something new and from inspiring people to pursue

a goal together. We both also enjoy contributing to society. This year, for instance, we organized the 'Tour de spotit' for the second time. The proceeds go to charity."

How do you divide roles between you?
Steven: "We are very complementary. I'm responsible for sales, finance, legal, and international strategy. Frederik handles everything related to technology, our portfolio, and which partnerships we should pursue."
Frederik: "We both believe that we're good at what we do and share values such as respect, honesty, and positivity."
Steven: "And we can discuss anything openly with each other."

Does that reflect in the company culture too? What is the 'spotit DNA'?
Frederik: "For potential employees, we consider it important that there's a match with our four core values: expertise, human to human, entrepreneurship, and trust. This isn't a company where everything is arranged from A to Z. People who can teach themselves new knowledge or skills have an advantage. That 'getting things done' mentality is decisive."
Steven: "People here get a lot of freedom, but also need to be able to take responsibility. We also expect them to come up with solutions to problems and to make decisions. Our motto is 'gazze geven'."
Frederik: "You can also see that in our flat organizational structure. We have a management team of four: the two of us, a Head of Operations, and a Head of Finance. Below that are teams that handle more operational tasks themselves. They are supported by an Operations Chief of Staff, who has a coaching role, and the HR coach. We ourselves are also very approachable: if someone has an idea, they can present it to our executive committee, where decisions are made quickly. We also strongly promote team spirit. Every month, we update staff about our activities, there's a team event every quarter, and we organize drinks and sports activities... All initiatives to make sure people enjoy coming to the office, get to know each other better, and therefore collaborate better."
Steven: "Our people are our most important assets. Without them, we are nothing. We're proud that we have the best people in networking and security. We even have our own academy where recently graduated IT professionals receive six months of training in both hard and soft skills."

How do you view growth?
Steven: "We actually don't have strict revenue and profit targets. We want to be a healthy company but most of all have satisfied customers. Our NPS score is an important KPI for employee bonuses."
Frederik: "Sustainable growth is much more than just making a profit. That's why we follow a vision that spans 5 to 10 years, not just 1 or 2."

Is that also why you remain the only shareholders?
Steven: "Yes, because when you bring a private equity partner on board, the focus is often more on the short term."
Frederik: "And then there's constant oversight on targets. That creates certain expectations and limits our freedom."
Steven: "We get many requests for talks about partnerships, but we're not open to that. We choose freedom and independence to chart our own course."

What are your ambitions for the coming years?
Steven: "We aim for healthy growth with good people. We're ready for that: our new generation SOC is fully complete, available as open source or Microsoft variant, and customers can count on our added value in service. Thanks to these elements, we are able to challenge the major players. We want to be the best, not the biggest."
Frederik: "We've become more cautious than before about making very ambitious statements, because the world changes so quickly—not just geopolitically, but also in terms of technology."
Steven: "Do we have international ambitions? We see opportunities in the Netherlands, Scandinavia, and Germany. We already have customers there and there's a cultural fit. If demand suddenly increases or if an acquisition becomes possible, our business there could gain momentum."

There are also many opportunities with your recent 'product' Cyberwolf. What exactly is that?
Steven: "Cyberwolf is essentially a 24/7 digital bodyguard for private life. It's intended for C-level, board members, ministers, magistrates, and wealthy individuals around the world. Essentially, we do for them what we do for businesses: identify vulnerabilities, detect fraud, track conversations on the dark web, and protect the client if something happens. For a major American company—which we can't name—we're already providing cybersecurity for their entire global leadership board. The potential is enormous."

Finally: AI is currently a hot topic. What trends do you see coming in the world of cybersecurity?
Frederik: "Artificial intelligence will definitely cause a shift in how we run security in the future. All the technologies we use already have AI built in, but there are still many opportunities. Together with KU Leuven and VUB, we've been doing research for years into applying AI in cybersecurity so we can make operations less dependent on people. We also share threat intelligence with the Centre for Cybersecurity Belgium, among others. Besides AI, the cloud remains a huge business accelerator, and companies are increasingly aware of the importance of OT security (in production environments). So much is still to come—and we are definitely ready for it!"

Who are Frederik and Steven?

Frederik Rasschaert (43) lives in Beveren-Waas, enjoys running and cycling (followed by good food and drinks), traveling, and spending time with friends. On weekends, you can often find him cheering for his two children on the football field.

Steven Vynckier (49) loves cycling (after he had to give up running), and enjoys playing cards with friends and family. He proudly supports his daughter who dances and his son who plays table tennis.

€30.000.000

Revenue Skyleaf (Spotit + Cyberwolf)

MOST POPULAR ASSESSMENTS IN 2024

- Pentest
- NIS2 Assessment
- Security & Network Assessment

10%

growth

FACTS &STATS

21

active customers (in portfolio)

4 SECTORS WHERE WE ARE MOST ACTIVE :

1. Utilities & Energy sector
2. Manufacturing & Process Industry
3. Logistics & Harbor
4. Pharmatech & Lifesciences

73% OF RISKS ORIGINATE FROM 3 MAIN IT DOMAINS (SOURCE: UNIT 42)

- IT & SECURITY INFRASTRUCTURE
- SERVICES FOR REMOTE ACCESS
- BUSINESS APPLICATIONS

TOP 3 ATTACKS BY VOLUME IN EUROPE (SOURCE: CCB)

RANSOMWARE | DATA THEFT | DDOS

TOP 3 ATTACKS BY VOLUME IN THE SPOTIT SOC

PHISHING | MALICIOUS CODE | INTRUSION (ATTEMPTS)

Insights into cyber threats in 2024

HOW DO THEY GET IN? MOST USED METHODS (SOURCE: SPOTIT CSIRT)

EXPLOIT | EXPOSED SECURITY INFRA | MALWARE

TOP 3 GREATEST THREATS IN BELGIUM (SOURCE: ENISA)

DDOS | RANSOMWARE | ACCOUNT COMPROMISE

MOST USED ATTACK LINKED TO MOTIVE IN EUROPE (SOURCE: ENISA)

- RANSOMWARE – FINANCIAL GAIN
- DDOS – IDEOLOGY
- MALWARE – ESPIONAGE

Aside from figures from the Centre for Cybersecurity Belgium, the following reports are also valuable sources:
Unit 42 Incident Response Report 2024 / Threat exposure Brucon 2024 / ENISA Threat Landscape 2024 / 2024 Report on the State of the Cybersecurity in the Union / Internet Organised Crime Threat Assessment IOCTA 2024 / Unit42 Attack Surface Threat Report / Verizon data breach report 2024

TRENDS AND CHALLENGES IN 2024

Cybersecurity and connectivity have become an inseparable duo at the heart of our digital society. Organizations that want to grow digitally are investing heavily in these two essential pillars. But there are also irreversible trends and serious challenges to consider. In 2024, we continued to closely monitor these developments.

1. The rise of artificial intelligence in cybersecurity
The use of artificial intelligence (AI) in cybersecurity is a game changer. AI algorithms are becoming increasingly advanced and are capable of detecting and responding to threats faster than humans ever could. AI even enables predictive analytics: the forecasting of potential vulnerabilities.

2. The evolution of edge computing
Edge computing is a revolution for connectivity by processing data closer to its source. This shift increases speed and improves reliability, but also introduces new challenges. Securing the wide variety of devices and data points at the edge requires innovative security approaches.

3. Zero trust security models
The concept of "never trust, always verify" has become a cornerstone of cybersecurity strategies. As remote work blurs the boundaries of traditional network perimeters, zero trust models ensure that security is based not on location, but on continuous verification of identity and access privileges.

4.The expansion of 5G
The rollout of 5G networks enables ultra-high bandwidth connectivity and an explosion of connected devices and applications. However, it also opens new paths for cyberattacks. Securing 5G networks and connected devices is essential to fully realize their potential.

5. Regulations and privacy
With the increasing frequency of data breaches, governments around the world are introducing stricter data protection laws. Companies must navigate this complex regulatory landscape to avoid heavy fines and reputational damage, while also protecting customer privacy. The recent NIS2 Directive is a concrete example, requiring companies and organizations to invest more in cybersecurity.

cybersecurity & networking

Wim Remes, Head of Operations at spotit, naturally agrees with the trends identified by Gartner. At the same time, he urges for a healthy dose of realism. His advice: start with the basics and grow step by step in digital maturity—with first-class connectivity and enhanced cybersecurity at every stage. Sounds simple, but it's not always easy. Wim highlights the following challenges:

1. Language
Executive teams and IT departments still too often speak different languages. Ensuring mutual understanding—standardizing the language—is a major challenge to ensure that the right information reaches the right people. This is especially urgent now that regulations like NIS2 make executives personally liable. Clear and unambiguous communication is a must.

2. People
Technology is a necessity and a useful tool, but people make the real difference. Experts with experience know how to act in critical moments. Keep people trained—organize regular tabletop exercises. This helps to ensure that incidents are handled efficiently and that everyone knows their role in the event of a major incident. Teamwork is essential.

3. Design
Today's IT infrastructure design must be Distributed, Immutable, and Ephemeral. This means various components must be able to interoperate, changes in a system must be detectable and controllable, and entire infrastructures or parts of them must be easily and safely refreshed. With the right setup, operations can continue on a trusted infrastructure as soon as a cyber incident is detected. Many companies are still in the early stages of this architecture transformation.

4. Data
Data is a massive challenge for many organizations. It's increasingly dispersed and growing exponentially. How do you store it? How do you make sense of it? In security operations, we're seeing a shift toward "data pipelines": a set of processes that move and transform data from one location (the source) to another (the destination). It's a key part of data engineering, especially in big data environments where vast volumes of data must be continuously processed and analyzed.

5. Regulations
New regulations like NIS2 and DORA (for the financial sector) are on the horizon. Tackle them pragmatically. For NIS2, Third Party Security Management—identifying your most critical suppliers—is the biggest challenge. Make sure your process is under control and work together with partners to secure the supply chain.

Want to discuss the latest trends and challenges in cybersecurity and connectivity with Wim? Don't hesitate to reach out.

Sources: Cybersecurity Trends 2024 to Safeguard your Digital Assets | Gartner - Top Cybersecurity Trends and Strategies for Securing the Future | Gartner - The NIS2 Directive: What Does It Mean for My Organization? | Centre for Cybersecurity Belgium

“Cloud technology has changed everything”

CTO FREDERIK ON THE IMPACT OF TECHNOLOGY

Eleven years ago, the digital world looked very different. Mobile internet was still in its infancy, and social networking was far less prevalent. Since then, digitization has grown exponentially, bringing both new opportunities and new risks. The number of cyberattacks has increased significantly because, quite simply, there are more ways to attack. People now own multiple devices (smartphones, tablets, laptops, smartwatches, etc.) and are constantly online.

When spotit started, the budgets for a Security Operations Center (SOC) were extremely high, which meant only a small portion of Belgian companies could invest in one. Today, we’re seeing a reversal: cybersecurity is now on every company’s radar. Moreover, technological advances have significantly reduced the cost of operating a SOC.

Cloud technology has fundamentally changed the way we work. Whereas everything used to run in on-premises data centers, now almost everything operates in the cloud. This means that security no longer revolves around a single physical location, but is distributed across multiple platforms and systems.

The way attackers operate has also changed dramatically. We are seeing more structured and state-sponsored cyberattacks. At the same time, frameworks like MITRE ATT&CK allow us to better map attackers’ tactics and link them to specific groups, such as those sponsored by Russia or North Korea. These insights help us defend more effectively than we could 10 years ago.

Until recently, security within Operational Technology (OT) was barely seen as a priority. Companies in these sectors were not open to cybersecurity involvement. That has changed: with the rise of IoT and the digitization of industrial processes, OT security has become a critical area of focus.

Artificial intelligence is playing an increasingly important role in cybersecurity. On the one hand, AI helps us secure systems better—for instance, by detecting suspicious activity more quickly and supporting security analysts. On the other hand, AI models themselves must also be protected. We help customers secure their AI systems against data breaches and misuse. Meanwhile, cybercriminals are also using AI to enhance their attacks.

Not only companies, but also individuals have become more vulnerable. Everything is now digital: photos, documents, emails, calendars, private conversations. Smartphones and laptops are always connected, increasing the risk of eavesdropping and espionage. This means that certain groups—such as business leaders, politicians, and other high-profile professionals—are at greater risk. Our role is to protect them better.

Corporate Social Responsibility

Environment

Last year, we took further steps to reduce our ecological footprint. Through conscious choices, we contribute to a more sustainable future. Our actions reflect our responsibility to the environment and to future generations.

- **E-waste:** we developed a policy to avoid unnecessary or careless printing.
- **Electrification of the vehicle fleet:** only fully electric cars are part of our car policy
- **Shared workspace and remote work:** by sharing resources/space and reducing emissions from commuting, we minimize our environmental impact.

Governance

Strong governance and transparency are key to sustainable success at spotit. Long-term value creation, integrity, and stakeholder engagement are therefore central in our decision-making. This further strengthens the bond of trust with our customers, partners, and employees.

- **External advisors:** the Skyleaf holding has an advisory board with external experts. They provide a fresh perspective on our strategy.
- **Optimized organizational structure:** as a growing company, we find it important to continuously adjust our organizational structure. In addition to the two CEOs and the executive committee, a management committee was introduced in 2024 with input from employees.
- **Close customer involvement:** we organize an annual qualitative survey of 50 to 75 customers. During a lunch session, we inform our ambassadors first about future plans and innovations. Also on next year's roadmap: the launch of a customer advisory board. A select group of customers will contribute to our strategic direction and roadmap.

Social

People are the core of our success. In 2024, we further focused on the development and well-being of our employees. By collaborating and connecting with other organizations such as higher education institutions, we create a positive impact both within and beyond our organization. We also support charitable causes.

- **Second edition van Tour de spotit:** on Saturday, April 27, we organized our second edition of the Tour de spotit. No fewer than 83 friends, family members, and employees gave their all and cycled a total of 6,300 kilometers. We raised €10,000 for the charity De Zelfmoordlijn.
- **Lifelong learning:** our spotit Academy reflects our commitment to training and coaching. Recent graduates can follow a six-month traineeship with training from internal and external coaches. In addition to theoretical lessons, they gain substantial hands-on experience. They learn not only essential IT technical skills but also soft skills such as planning and communication. Naturally, training and continuous development remain high on the agenda for our more experienced employees.
- **Sharing knowledge with schools:** we've partnered for several years with KU Leuven and VUB, working on projects related to AI in cybersecurity.
- **Focus on diversity and inclusion:** in a sector like ours, achieving a balanced gender ratio is not easy, but it's a topic we consciously address. Currently, 17% of our employees are women. Fun fact: our team includes not only Belgian employees, but also colleagues from the U.S. and Italy.

Spotit's 360° evaluation cycle

THE POWER OF FEEDBACK

At spotit, we believe growth comes from honest and constructive feedback. That's why we use a 360° evaluation cycle that goes beyond traditional top-down assessments. In our approach, every voice counts: team leads evaluate team members, colleagues give each other valuable feedback, and employees have the opportunity to share their opinions about their team lead.

This holistic method fosters a culture of trust, transparency, and collaboration. It ensures everyone has a clear view of their strengths and areas for growth. By collecting feedback from all those you work with, we aim to empower individuals, grow teams, and excel together. Because at spotit, growth is not a solo journey—it's a team effort.

Multiple perspectives at the table

Every October, we launch our annual evaluation cycle with peer feedback. These colleagues may be direct teammates or people from other teams involved in specific projects. Employees can select three to five colleagues to gain valuable insights into their skills, communication, and collaboration.

Next comes feedback from their team lead, who assesses them based on a range of professional and soft skills, as well as spotit's core values. Employees also get the chance to evaluate their team lead—because good leadership starts with listening and incorporating feedback.

All information is stored in each employee's profile in our evaluation tool, which we also use to track goals. Employees can always review their evaluations and objectives.

All this input is discussed in a meeting with their manager. It's the perfect time to clarify expectations, explore opportunities, and collaboratively shape a personal growth path.

CASE

Belgian Federation of Food Banks

Since recently, the Belgian Federation of Food Banks has a **brand-new, secure, and high-performance network.** As a result, the distribution of food packages to those in need is now much more efficient—much to the satisfaction of the food bank volunteers.

Since COVID-19 and the energy crisis, the volume of food packages increased so dramatically that it became impossible for volunteers to manually count inventory. With an automated system using barcode scanners, they can now work more efficiently, reduce errors, and ensure accurate reporting to the government. To make this system possible, a **stable and secure network** was essential.

Cisco donated the network hardware, but of course, that hardware also needs to be installed, **managed, and monitored 24/7.** Spotit's Security & Network Engineers rolled out new networks in the warehouses and integrated them into the spotit NOC. This enables them to respond quickly and intervene when alerts from network devices are triggered. Food Bank Limburg now has a professional network with 15 access points covering the entire warehouse with stable and secure Wi-Fi. Additional devices such as burglar alarms and surveillance cameras were also connected to the network.

"I truly recommend spotit! There's no doubt about it. They handle their clients very well and remain constantly vigilant."

Bart Buckinx, Managing Director of Food Bank Limburg vzw

“The spotit Academy gives you a real head start”

PARTICIPANT EMILE TRENSON

Since the launch of the spotit Academy five years ago, more than 30 young professionals have graduated—85% of whom are still working at spotit today. In the six-month traineeship, promising talents receive training from internal and external coaches. Emile Trenson, now active in the spotit SOC, shares his experience.

What’s your background?
““I studied Electronics-ICT at Odisee University College, specializing in infrastructure. At a job fair, I came into contact with spotit. A lot of companies try to attract you with flashy booths, but that wasn’t what I was looking for. When I spoke with the people from spotit, I immediately felt a click with their approach and culture. That’s how my interest grew.”

You participated in the spotit Academy in 2019–2020. What exactly is it?
“When spotit noticed it was hard to find experienced employees, they decided to train newcomers themselves. School leavers or people making a career switch can apply for the Academy. Not just their prior knowledge, but especially their motivation and fit with the company are decisive. If accepted, they follow a six-month program that elevates their IT knowledge. The first two to three months focus entirely on theoretical knowledge. Then, staging assignments and lab exercises are added. This way, participants can test their knowledge in practice, guided by a mentor. One component, for example, is learning to build a network from scratch, rather than just adjusting existing systems. In addition to technical training, there are also soft skills courses, such as time management and client-focused communication.”

How do you look back on your participation?
“Very positively. The Academy gives you the chance to acquire a lot of knowledge in a short time—something that would otherwise take much longer. Many companies only gradually entrust newcomers with responsibilities, whereas I was really prepped at spotit and quickly got to work. A true head start! I think very few participants have regrets—many of them stay with spotit for a long time. For the past three years, I’ve been involved in organizing the Academy myself. From my experience as a security analyst, I help new participants with their journey. For example, I guide them through the lab exercises.”

Finally: how would you summarize the spotit Academy?
“A unique opportunity that gives a lot in return! With the Academy, the company truly invests in young talent. That’s not a given. It shows you’re trusted here.”

What is the spotit Academy?

Promising talents can follow a six-month traineeship filled with training by internal and external coaches. In addition to theoretical classes, hands-on practice is also part of the program. We teach participants not only the necessary IT technical skills but also focus on soft skills like planning and communication. Ideal for starting a successful career in security & networking—and for growing within spotit over the long term. The seventh edition starts in September 2025.

Outstanding performance thanks to a strong team

Every day, our employees help build the future of our organization and our customers. Get to know our various teams:

MANAGED SERVICES

- **SOC team:** our Security Operations Center monitors and protects customers' IT environments 24/7 against threats, with real-time detection and response.
- **CSIRT:** a separate team that reacts quickly and expertly to security incidents to minimize damage.
- **NOC team:** manages and optimizes network performance and uptime with a proactive and problem-solving approach.

DOMAIN EXPERTS

- **OT team:** focuses on the security and connectivity of industrial systems, with expertise in unique OT challenges.
- **Offensive team:** conducts ethical hack tests and vulnerability analyses to strengthen systems against potential attacks.
- **Consulting team:** helps organizations manage risks, ensure compliance, and develop a strong security strategy.

TECHNOLOGY

- **Internal IT Operations team:** ensures our employees have the best tools to deliver productive and high-quality work.
- **Service Excellence-team:** combines development and operational expertise to deliver fast, reliable, and scalable solutions. The team consists of: **DevOps** (automates repetitive processes and tasks to benefit clients and spotit colleagues), **Data Science** (analyzes existing data (client or spotit) and turns it into useful reports) and **Platformation** (sets up the IT ticketing system and continuously improves ticket handling).

OPERATIONS

- **Architects team:** translates network and security challenges into tailored technological solutions.
- **Projects & Service Management team:** implements custom solutions for complex IT projects, from start to finish, with a focus on quality.
- **Security Engineering team:** the go-to team for the most complex security issues.

SALES & MARKETING

- **Presales, Sales & Marketing, Service Development team**: connects customer needs with spotit solutions through a customer-focused approach and compelling communication.

STAFF

- **HR team:** committed to attracting, developing, and supporting talent, with a focus on a stimulating and positive work culture.
- **Finance & Orders team:** ensures financial stability and growth with accurate planning, analyses, and strategic management.
- **Legal:** good agreements (on paper) make good partners.
- **Facilities & Reception:** provides an excellent office environment and a warm welcome.

Our Partner Ecosystem

"If you want to go fast, go alone. If you want to go far, go together." And we especially want to go far – together. That's why we invest a lot of time and resources in setting up and maintaining strong, sustainable partnerships.

Our strategic technology partners

We believe in the power of collaboration. That's why we deliberately choose technology partners who are leaders in their sector. Each one combines innovation and quality and, like us, aims for sustainable solutions. With these strategic alliances, we build long-term relationships that benefit our clients – today and tomorrow.

Our academic partners, sector federations, and network organizations

As specialists in cybersecurity and networking, we take our role in the broader ecosystem seriously. Through our membership in organizations, we stay up to date on technological and policy developments and actively contribute to the future of the sector. In doing so, we help build a strong, innovative, and resilient business climate.

Our valued clients

Many companies in Belgium rely on us. And we're proud of that!
Here's a selection:

Take a look at some of our references

Ready to discuss your network and security needs?

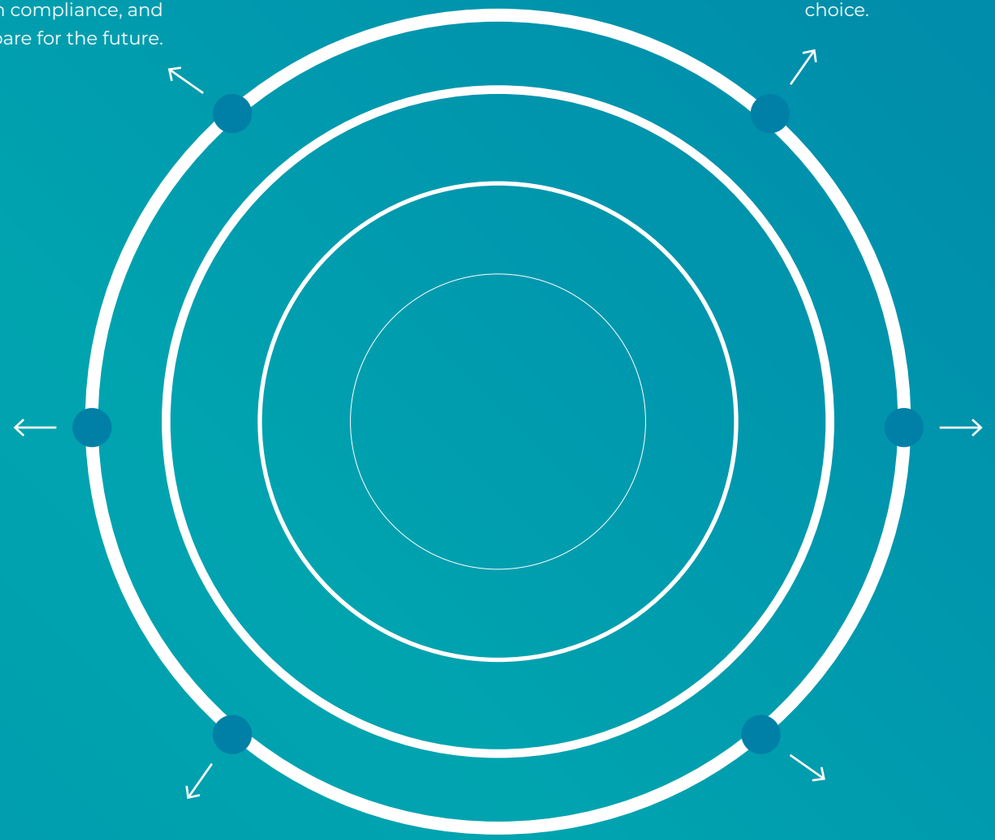
We're always available. Don't hesitate to contact us for an informal conversation and a good cup of coffee. Visit us at one of our offices or schedule a meeting with an expert.

www.spotit.be
+32 (0)9 322 04 44
info@spotit.be

Key focus areas for the future

Stronger focus on governance, risk & compliance
Governance, risk management, and compliance (GRC) have long been an integral part of our service offering. With an **experienced team of specialists**, we support clients across various sectors. Today, GRC is gaining momentum – especially with the arrival of NIS2 and increasingly stringent regulations. That's why we're investing strategically in expanding our GRC activities. In doing so, we remain a reliable partner for companies aiming to control risks, strengthen compliance, and prepare for the future.

Peace of mind thanks to our 100% Belgian SOC and NOC
For ten years, we have distinguished ourselves with a **unique combination of a SOC (Security Operations Center) and NOC (Network Operations Center).** While many providers focus solely on cybersecurity, we also offer the underlying network expertise that is essential for a robust security approach. After all, true security starts with a stable, high-performance network. Moreover, all our services are **100% Belgian**. In times of geopolitical uncertainty, that's a reassuring factor for many clients – and a deliberate choice.



Accelerating OT Security & Networking
Operational technology is the beating heart of sectors such as logistics, industry, utilities, and pharma/life sciences. Yet OT networks often don't receive the attention they deserve. To change that, **we are fully committing to OT Security & Networking** with a dedicated business unit. This enables us to offer our clients the specialized knowledge, approach, and technology needed to make their operational systems future-proof and cybersecure.

Strong growth in the public sector
Until recently, we were less visible in the public sector – but that's changing quickly. We are now actively pursuing **partnerships with governments and organizations in healthcare and education.** A key milestone is our partnership with Shield vzw, a consortium that supports healthcare institutions and higher education organizations in setting up and managing a high-performance, secure cybersecurity architecture. With our solutions and expertise, we're helping to build a digital and resilient public sector.

Rapid and effective support during cyber crises
With our CSIRT team (Cyber Security Incident Response Team), we are ready to assist companies during digital incidents and crisis situations. But we're going one step further. **We're expanding our offering with offensive security**, where we simulate targeted attacks – always in consultation with the client – to uncover vulnerabilities before real hackers do. For this new business unit, we have appointed an experienced expert to help proactively arm our clients against cyber threats.

Cyberwolf accelerates internationally
Over the past few years, Cyberwolf has built a strong client portfolio in both North America and Europe. We are now aiming to accelerate that **international growth**. Until now, we have consciously operated under the radar. But the next step is clear: increasing our visibility – without losing our hallmark discretion. Cyberwolf remains a silent force – but one that is making an ever-greater impact.


spotit
YOUR SECURITY & NETWORK LAYER