GUIDE

spotit
YOUR SECURITY & NETWORK LAYER

Always On, Always Protected:

A Practical FAQ Guide to Managed SOC Services

Executive Summary

Cyber threats evolve faster than most organizations can keep up with. Attackers work around the clock, exploiting every gap, from unmonitored endpoints to cloud misconfigurations and vulnerable OT systems. For many companies, even those with mature IT teams, **maintaining continuous visibility and a fast, expert-led response to incidents has become increasingly difficult. The need for a Security Operations Center (SOC) has never been clearer**, yet building one internally requires significant investments in technology, specialized talent, and 24/7 staffing.

A Managed Security Operations Center (Managed SOC) bridges this gap by delivering continuous monitoring, rapid detection, and expert response as a fully managed service. It acts as an extension of your security team: **watching over your IT and OT environments day and night, detecting suspicious activity before it becomes a crisis, and responding immediately when an attack occurs.** This proactive, always-on protection dramatically reduces the likelihood of damage, downtime, and regulatory exposure.

This **FAQ guide** explains what a Managed SOC is, how it works, and why so many organizations, across sizes and sectors, turn to external SOC providers like spotit to strengthen their cybersecurity posture. It covers the practical benefits such as cost efficiency, access to advanced technologies, 24/7 vigilance, and support for compliance frameworks including ISO 27001, GDPR, and NIS2. It also clarifies **how a Managed SOC collaborates with your internal teams**, scales with your business, and compares to operating an in-house SOC.

Finally, the document highlights spotit's Managed SOC, built on more than a decade of cybersecurity expertise. With a multidisciplinary team, a technology-agnostic approach, strong automation capabilities, and deep experience across IT and OT environments, spotit delivers a SOC service focused on fast response, measurable outcomes, and continuous improvement. Whether you need full 24/7 detection and response or want to elevate your existing security maturity, spotit's **SOC offers the flexibility, expertise, and reliability to protect your business today and prepare it for tomorrow's threats**.

This FAQ serves as your guide to understanding the value, workings, and strategic impact of a Managed SOC and why it has become a cornerstone of modern cyber resilience.

The 10 most Frequently Asked Questions about Managed SOC

02

1

What is a managed Security Operations Center (SOC)?

A Managed SOC is an outsourced cybersecurity operations team that watches over your IT and OT environment 24/7 to detect and respond to threats. Think of it as a remote security control room for your organization's digital environment.

The Managed SOC's experts use specialized tools to monitor your users, networks, servers, cloud services and devices around the clock. If they spot anything suspicious, like signs of a hacker or malware, they investigate immediately and take action to contain the threat.

2

Why would my organization need a managed SOC?

Cyber attacks can strike any organization, big or small, and at any time. Many businesses have basic defenses but still struggle to catch advanced threats or attacks that happen outside office hours. A Managed SOC addresses this gap by providing constant vigilance and expert response. For example, if a new ransomware variant tries to infiltrate your network overnight, the SOC team is there to catch it before it spreads. Organizations choose Managed SOC services because they offer a proactive approach to security rather than waiting to discover a breach days or weeks later, the SOC is actively looking for threats in real time. This significantly reduces the risk of serious damage, downtime, or data loss. If you don't have the resources for a full internal SOC, or want to strengthen your security posture, a Managed SOC provides peace of mind that professionals are actively protecting your business around the clock.

3

What are the main benefits of using a managed SOC service?

Continuous 24/7 Monitoring: Your organization is watched day and night, weekday or weekend. This means threats are caught immediately, even at 3 AM on a Sunday, drastically reducing response times and potential damage.

Expert Incident Response: You have a dedicated team of trained cybersecurity experts ready to jump into action when an incident occurs. They know how to analyze alerts, contain attacks, and remediate issues. This expertise vastly improves your ability to handle incidents effectively compared to ad-hoc in-house efforts.

Cost-Effective Security: Instead of investing heavily in building your own SOC (hiring full-time analysts, buying expensive monitoring tools, etc.), you pay for a managed service. Costs are spread out among the provider's clients, so you get enterprise-grade security at a fraction of the price of doing it yourself.

Access to Advanced Tools & Intelligence: Managed SOC providers use sophisticated security tools, threat intelligence feeds, and automation. You benefit from up-to-date technologies and global threat insights without managing them directly. The SOC can spot emerging threats (including new viruses or hacker tactics) that your basic security tools might miss.

Helps Meet Compliance: The service typically includes detailed logging, reports, and on-demand expertise to help you meet regulatory or industry security requirements. For instance, a Managed SOC can help demonstrate compliance with standards like ISO 27001, GDPR, or NIS2, by providing evidence of continuous monitoring and incident response processes.

Frees Up Your IT Team: With an external team handling the tedious and time-consuming task of security monitoring, your internal IT or security staff can focus on their primary job duties and projects. The SOC filters out false alarms and handles real threats, lightening the load on your team and letting them concentrate on core business needs.

4 Do we really need 24/7 monitoring? What if we only operate during business hours?

24/7 monitoring is crucial because cyber threats can occur at any time, not just 9–5. Attackers often strike during off-hours when organizations are less likely to notice much like a burglar preferring to break in at night. If you only watch during business hours, an attack at midnight might go undetected for many hours, allowing it to spread or do significant harm.

A Managed SOC's round-the-clock monitoring ensures that even at 2 AM on a bank holiday, there are eyes on your organization and an expert ready to respond. This is especially important given the global nature of cyber-attacks. While it's nighttime for you, it might be daytime for a hacker on the other side of the world.

Continuous monitoring means your security never "clocks out." It provides assurance that threats will be caught and addressed in real time, minimizing damage.

5 How does a managed SOC respond to security incidents or attacks?

When a potential security incident is detected, a Managed SOC will act immediately according to a well-defined incident response process.

First, the tooling might automatically flag unusual behavior (for example, a surge in failed logins or malware detected on a PC). A SOC analyst then investigates the alert to confirm if it's a real threat. If it is an attack or serious issue, the SOC team will quickly work to contain the threat. For instance, isolating an infected machine from the network, blocking malicious IP addresses or emails, and stopping the spread of malware.

They'll notify your organizations designated contacts about what's happening, typically providing details and guidance on next steps. The Managed SOC can often neutralize or mitigate the attack directly through remote actions or by guiding your staff on what to do, thereby reducing harm. After containment, they'll assist in cleaning up (removing the threat, patching vulnerabilities) and recovering any affected systems. the SOC will provide an incident report explaining what happened and recommendations to prevent similar incidents. This fast and expert-led response means even if a breach occurs, it's handled swiftly and systematically, limiting damage and downtime for your business.

6 Is a managed SOC cost-effective compared to building an in-house SOC?

A Managed SOC is far more cost-effective than creating an in-house SOC from scratch. Building your own SOC requires major upfront and ongoing expenses. You'd need to purchase security monitoring tools , set up infrastructure to handle large volumes of log data, and hire a team of skilled analysts to staff 24/7. Beyond salaries, there are costs for continuous training, threat intelligence subscriptions, and maintaining the technology. These expenses quickly add up for a fully functional internal SOC. Many businesses simply cannot afford or justify that level of spending.

By contrast, a Managed SOC is provided for a predictable subscription fee, which is a fraction of the cost because the provider can spread the operational costs across many clients. You essentially share the expense of the high-end tools and expert staff with others. There's no need for capital investment on your side or hiring multiple new employees. In addition, the provider takes care of keeping the technology updated and the analysts trained, saving you money on continuous improvements. In short, you get a high-quality security operation without the hefty price tag of doing it all yourself. This makes advanced security monitoring attainable even for smaller organizations with limited budgets. Plus, avoiding a major cyber incident through effective monitoring can itself save enormous costs related to breaches (which can include fines, recovery costs, and reputation damage), making a Managed SOC a wise financial choice as well as a security one.

7 How can a managed SOC help with compliance and regulatory requirements?

A Managed SOC can be a big help in meeting various compliance, legal, and regulatory obligations related to cybersecurity. Many regulations and standards such as the GDPR, ISO/IEC 27001, NIS2 require organizations to have strong security monitoring, incident response plans, and audit logs. A Managed SOC service provides the continuous monitoring and documented processes that these standards call for. For example, the SOC will maintain detailed logs of security events and how they were handled, which is exactly the kind of evidence auditors look for when assessing compliance. If you need to demonstrate that you monitor access to sensitive data or respond promptly to incidents, the SOC's activity reports and incident summaries serve as proof.

Moreover, Managed SOC providers have expertise in compliance themselves, so they can tune the monitoring to your compliance needs. They might set up specific alerts for policy violations (like unauthorized data access), or provide regular reports mapped to compliance controls.

8 Will a managed SOC replace our internal IT or security team or how do they work together?

A Managed SOC is not a replacement for your internal IT or security staff. Rather, it's a valuable extension and support for them. Your internal team still manages day-to-day IT operations and makes strategic decisions about security (like what needs protecting most, approving changes, etc.), while the SOC team focuses on the continuous monitoring and immediate threat response piece. The two groups work in partnership: the SOC monitors and investigates issues, and they will contain or engage your staff when needed. For instance, if the SOC detects a serious incident, they will contact your designated people to inform them of the situation and possibly coordinate on response.

In a Managed SOC arrangement, you define escalation procedures and communication channels during onboarding. This ensures the SOC knows whom to reach out for various scenarios, and your team knows what to expect. The goal is that the SOC handles the heavy lifting of threat detection and initial analysis, freeing your team so they can focus on other projects. But whenever the SOC needs a decision (like whether to shut down a system) or once an incident is contained, they loop in your team to keep everyone informed. Many companies find that their internal IT folks appreciate having the SOC cover the overnight and technical monitoring tasks, as it reduces burnout and lets them be more effective in their normal roles.

9 Can a managed SOC service scale with my business as it grows or changes?

Managed SOC services are designed to be scalable and flexible. Whether your business grows in size, adopts new technologies, or expands into new regions, a good Managed SOC can adjust its coverage to match. If you add more offices, users, or IT systems, the SOC can onboard those new data sources into their monitoring tools, so everything stays protected. Likewise, if you move more assets to the cloud or start using new platforms, the provider can incorporate those into the monitoring scope. This scalability is typically built into the service model: you might start with monitoring a certain number of devices or log sources and then increase that number as needed (usually the pricing will adjust based on usage or number of endpoints, for example).

Because the SOC provider already operates a full 24/7 operation, adding extra capacity or adjusting to your needs is usually seamless on your end. You inform them of changes, and they allocate more resources behind the scenes.

This is much faster and easier than trying to scale an in-house SOC, where you'd have to hire additional staff or buy more servers/software for yourself. Additionally, if your security needs change (say, you need to meet a new compliance requirement or you want to enable additional services like threat hunting), managed providers often offer different tiers or add-on services that can be integrated without a huge effort.

A managed SOC grows with you: it's as suitable for a mid-sized company as it is for a large enterprise and can adapt as your organizations' risk profile and IT environment evolve. This means you won't outgrow the service. It can accommodate your needs from a small setup to a very broad, complex infrastructure, all under the same umbrella of consistent protection.

10 How does a managed SOC compare to having an in-house SOC?

Managed SOC and an in-house SOC ultimately aim to do the same job (continuous security monitoring and incident response), but they differ in execution, cost, and convenience:

Cost and Resources: An in-house SOC requires substantial investment in tools, technology, and full-time personnel. You bear all the costs of salaries, training, and infrastructure. A Managed SOC, on the other hand, is paid via a service fee, and the provider supplies the technology platform and expert staff.

This makes Managed SOC much more cost-efficient for most businesses, since you're sharing those resources with other clients and don't need to fund everything yourself.

Expertise and Skills: When you outsource a Managed SOC, you gain access to a team of security experts with a broad range of skills and experience. Building an equally skilled in-house team can be very challenging due to the current shortage of cybersecurity talent. It might be hard to hire and retain the right people.

With a Managed SOC, the provider takes care of staffing and keeps their team's skills sharp.

Deployment Speed and Updates: A Managed SOC can typically get up and running faster. Providers have ready-made platforms and procedures, so they can onboard your organisation in weeks, whereas building an in-house SOC could take many months (hiring staff, setting up systems, etc.). Additionally, the provider will continually update their detection methods and tools as threats evolve, whereas an internal team might struggle to keep pace with rapidly changing technology.

24/7 Coverage and Scalability: Ensuring true 24/7 coverage in-house means hiring multiple shifts of analysts often not feasible except for very large companies. Managed SOCs deliver 24/7 by default, and scaling that coverage (up or down) is easier since they already operate at scale.

Control and Customization: An in-house SOC gives you direct control over every aspect of security monitoring and data storage. Some organizations prefer this for sensitive environments. Managed SOC involves entrusting a third-party with your security data and response. Good Managed SOC providers will still let you customize the service. For example, setting specific alert priorities or data handling policies but you are leveraging their predefined processes and tools.

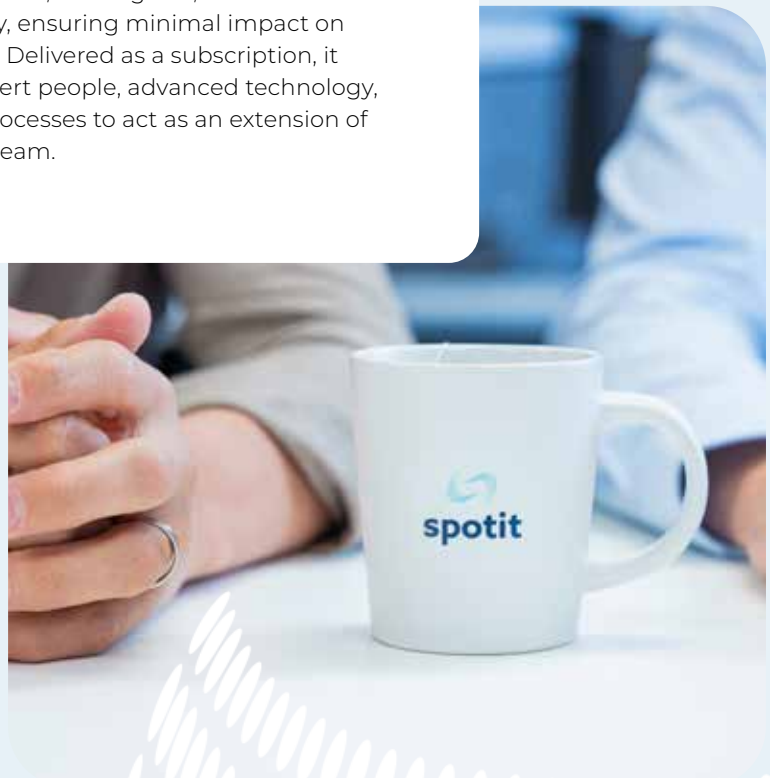
Focus on Core Business: Running an in-house SOC means you're in the business of cybersecurity operations, which can divert focus from your core mission. By using a Managed SOC, you let an external specialist handle the complexity of security ops, so your company's leadership and IT team can focus on strategic initiatives and your core business activities.

What makes the Security Operations Center of spotit unique?

03

What is spotit's Security Operations Center service?

Spotit's Managed SOC is a 24/7 security monitoring and incident response service that protects your IT and OT environments. The SOC team detects, investigates, and neutralizes threats quickly, ensuring minimal impact on your business. Delivered as a subscription, it combines expert people, advanced technology, and proven processes to act as an extension of your security team.



What benefits and value does spotit's SOC offer to clients?

24/7 Monitoring and fast response
Spotit provides continuous monitoring and immediate response to security incidents, ensuring threats are contained before escalation.

High degree of automation for efficiency
Automation and AI filter noise and enrich alerts, enabling faster detection and resolution while experts focus on critical issues.

Customized & scalable service
The SOC adapts to your business needs and scales as you grow, offering tailored solutions instead of one-size-fits-all.

Professional multi-disciplinary team support
You gain access to a full team of experts, including SOC analysts, incident responders, advisors and ethical hackers for comprehensive managed cybersecurity services.

Continuous improvement of security posture
Spotit proactively enhances your defenses through threat hunting, simulated attacks, and regular maturity assessments.

Alignment with your business & strategy
The SOC integrates with your processes, provides governance support, and ensures transparency through reports and reviews.

spotit
YOUR SECURITY & NETWORK LAYER

Why choose spotit's Managed SOC over other SOC providers?

- **Security expertise**
  Spotit is a specialized cybersecurity provider with over 125 experts and a strong track record as Belgium's largest independent MSSP.

- **Tailored, local service**
  Services are delivered from Belgium with dedicated roles for close collaboration, ensuring trust and cultural alignment.

- **Open, technology-independent platform**
  Spotit avoids vendor lock-in, integrating with any tools you use for maximum flexibility and cost efficiency.

- **Heavy automation & expert Focus**
  Advanced automation removes low-level tasks, so skilled analysts handle critical alerts for faster, more accurate responses.

- **Expanded services & continuous Improvement**
  Beyond monitoring, Spotit offers CSIRT support, governance expertise, and regular security enhancements as part of the SOC service.

Got hacked? Contact us 24/7
+32 (0)9 322 04 35

spotit
YOUR SECURITY & NETWORK LAYER