kaspersky

Getting it right the first time: SOC deployment without regrets

Introduction: when is it the right time to build a SOC?

There is no universal lightbulb moment when organizations realize they need a security operations center (SOC). Businesses, like people, are distinct entities that navigate unique challenges and mature at different rates. Nowhere is this truer than cybersecurity, with digital transformation and technological complexity inviting new risks over time – from mitigating targeted attacks to maintaining compliance on a global scale.

There are, however, common triggers that set the SOC-creation process in motion. Some of these are logical and proactive, including:

Regulatory requirements – especially in critical infrastructure

Proactive risk awareness – understanding that business can be interrupted by cyberattacks

Observed increase in cyberthreats – facing more frequent and/or sophisticated cyberattacks that require a dedicated team to mitigate

Some other triggers are reactive and therefore less desirable. One example is an attacked business realizing they didn't have the capability to respond effectively. They may start their SOC journey from a position of financial insecurity – and fighting to undo reputational damage.

> The most regrettable reason to start a SOC is that the company has suffered an incident and faced the consequences. The proper way is when you understand you can be attacked – and prepare before it happens.

Roman Nazarov, Head of SOC Consulting at Kaspersky

Data breaches, it's worth noting, often cost organizations millions of dollars – but such high figures are less likely for organizations using AI and automation heavily in their defense.

Clearly, it is more economically viable to build a SOC proactively than discover your security controls are insufficient amid an attack.

Core competencies required from day one

Once your organization has identified that it needs a SOC and has confirmed that it's possible financially, it's crucial that it begins on the right foot. This means identifying what's required for the SOC to function early – and building the foundations from which you can scale.

At the top of the list is human capability: every SOC relies on three core roles and without them success isn't possible:

Security analysts (investigation, triage and response) – frontline defenders who triage alerts, investigate suspicious activity and perform initial response. They separate false positives from real threats and ensure swift, effective incident handling.

Engineers (technical maintenance and support) – responsible for deploying, maintaining and optimizing security tools and infrastructure. They ensure systems like security information and event management (SIEM), threat intelligence platforms (TIP), and security orchestration, automation and response (SOAR) are functioning and scalable.

Threat researchers (modern threat awareness, detection development) – focused on identifying emerging threats and developing detection strategies. They analyze threat intelligence, create detection rules and help the SOC stay ahead of evolving tactics.

These roles cover **operations**, **technical maintenance** and **development for threat protection**. Each of them requires unique expertise that a fledgling SOC will fail without.

> The three core competencies for any SOC are security analysts, engineers and threat researchers. All of them need to be aware of modern threats and be prepared to fight them.

Roman Nazarov, Head of SOC Consulting at Kaspersky

But while these hires are crucial, they are not simple. Staffing SOCs with the right experience and expertise is being complicated by the cybersecurity skills gap, with an estimated four-million-person shortage globally.[1] And summing the market up: just 14% of organizations believe they have the people and skills needed to meet their cybersecurity objectives.[2]

This means you should factor in substantial time and budget when sourcing talent.

[1] World Economic Forum, Why Closing the Cyber Skills Gap Requires a Collaborative Approach, (World Economic Forum, 2024).

[2] World Economic Forum, Global Cybersecurity Outlook 2025, (World Economic Forum, 2025).

SOC viability and preparing to scale

We've discussed the skills and expertise required in a SOC, but headcount is also important. The minimum viable SOC is around ten to 12 people. Why? Because a SOC requires 24/7 coverage, with a foundational team of at least ten: a manager, five analysts, two engineers, and two researchers.

Small teams quickly face unsustainable workloads and alert fatigue (and many of the alerts may be false positives). This can lead to staff burnout and thus increase the likelihood of missed threats. It is not abnormal for IT-security professionals to make burnout-related errors that lead to security breaches.

Manpower is clearly important. If an organization doesn't have the means to staff its SOC appropriately, it's better off seeking an external provider that can perform threat monitoring on its behalf (more on this later). But if your business is in a position to start building its SOC, the focus shifts to scalability. Ensuring your technologies can scale horizontally, such as telemetry pipelines, correlation engines and other core systems, becomes critical. It's also important to anticipate architectural limits early on, so that you are prepared for growth and can account for future needs, such as disaster-recovery costs.

SOC shortcuts that work (and one that doesn't)

As with most business ventures, you can take some shortcuts to reach your goal – in this case SOC functionality – faster. One is to leverage third-party knowledge in the form of frameworks, which act as a blueprint for your SOC and can accelerate the design process. You can take their defined processes, adapt them to your infrastructure and get to work.

The next is not exactly short but will save you time in the long run, and that's continuous tuning and detection engineering, which is essential for preventing alert floods. Your technology must be tuned, especially default content, and adapted to your unique infrastructure. This requires clear processes for detection engineering and ongoing refinement of detection logic.

> You can't just implement security tools for monitoring like SIEM without tuning them and think that this would help you fight threats. You have to tune everything and adapt it to your infrastructure.

Roman Nazarov, Head of SOC Consulting at Kaspersky

Relying too heavily on default content will lead to excessive false positives. This is a big issue for SOC teams because it creates overwhelming noise that can obscure the signs of a genuine attack.

Long-term resilience requires continuous reviewing, refining and alert validation against real incidents.

Processes you must establish to ensure value

A successful SOC knows how to deploy not only people and tech but also processes – and there's an order in which these should come.

1

Inventorization of infrastructure – a major issue for many SOCs is that they don't understand what they're protecting. Inventorization may be IT-related, but it's a key SOC process because you must know what to protect in order to secure it. Understanding your protected infrastructure is key to defining how you can be attacked – enabling you to implement detection and prevention controls proactively.

2

Threat monitoring – the SOC itself should start with security monitoring. You must iron out how you acquire telemetry, detect signs of threats, and then manage those threats.

3

Mature operations – you should then switch to more advanced activities such as threat hunting, research and continuous detection engineering. Growing human expertise should also become a priority, as should establishing defined processes, deploying metrics, investing in SOC infrastructure resilience and maintaining continuous improvement.

Building a SOC requires this structured approach, starting with inventorization of infrastructure to ensure you know exactly what you're protecting. Security monitoring then becomes the focus. And as your SOC matures, you should prioritize the refinement of operations and integration of advanced capabilities. Each step builds on the last.

> The very first thing you do should be inventorization. Many SOCs discover years later that they are monitoring only part of their infrastructure.

Roman Nazarov, Head of SOC Consulting at Kaspersky

When to bring in MSSPs and external consultants

MSSPs

Not every business should build its own SOC. Those lacking the time, desire or resources to build one should consider a managed security service provider (MSSP). This is a third party who can deliver monitoring and incident response suited to the organization's industry, capability and budget.

For large enterprises, MSSPs can provide detection content during the creation of an in-house SOC, which typically takes nine-plus months. They can also help to bridge the skills gap, acting as a placeholder while your SOC is being staffed and trained.

They can also be incorporated in a phased handover model: you run operations jointly for 6–12 months, learning from your MSSP, before eventually going fully in-house.

External consultants

It's a good idea to bring in external consultants from the beginning of your SOC journey to prevent potentially costly mistakes. They can provide tested approaches and design that have already been proven in similar environments and share insights on what works and what doesn't, showing you how to adapt SOC processes effectively.

Preparing for and measuring SOC success

A SOC must deliver value early. You should prepare with clear objectives, defined playbooks and the right people, processes and technology. It's crucial to prove readiness through rigorous testing – one method is red team drills to validate detection of every attack stage, and drills and attack simulations to confirm full coverage. These exercises can expose (and help you close) gaps before real incidents occur.

You can measure your SOC's success using mean time to detect (MTTD) and mean time to respond (MTTR). Falling MTTD shows faster threat discovery, while lower MTTR proves quicker containment and remediation. Constant testing and metric tracking will ensure your SOC is improving from day one.

Common mistakes in first-time SOCs

First-time SOCs often rely too heavily on technology and default vendor content, assuming that tools will function effectively without tuning or skilled operators. Expecting instant results from out-of-the-box solutions leads to missed threats and false confidence. Do not make this mistake.

Another common pitfall is neglecting continuous improvement – treating the SOC as static rather than an evolving capability, which prevents adaptation to new attack techniques.

> The most common mistake is to consider SOC detection technologies as black-box solutions that don't require tuning and adaptation.

Roman Nazarov, Head of SOC Consulting at Kaspersky

Key takeaways

A successful SOC starts with a core team of analysts, engineers and researchers. Frameworks can accelerate setup – but tuning and customization are essential. You should start with asset inventorization, understanding of the possible attack vector, and basic monitoring before implementing advanced processes. MSSPs and consultants can support early operations, help to bridge your skill gaps and provide ongoing expertise.

Remember: it's important to plan for scalability from day one, considering both technology and budget. Above all, people are critical. Without sufficient human capacity and expertise, even the best tools and frameworks will not prevent SOC failure.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. With over a billion devices protected to date from emerging cyberthreats and targeted attacks, Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection, specialized security products and services, as well as Cyber Immune solutions to fight sophisticated and evolving digital threats. We help over 200,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

www.kaspersky.com

© 2025 AO Kaspersky Lab.
Registered trademarks and service marks are the property of their respective owners.