People, processes, technology: building a successful Security Operations Center

kaspersky BRING ON THE FUTURE

The rise of the SOC

Security Operations Centers (SOCs) are an increasingly popular way for organizations to secure themselves from cyberattack by centralizing personnel, tools and expertise as a single department that operates round the clock. This approach has many advantages, including reducing the fragmentation of traditional IT security while turning cybersecurity into a cost center whose performance and return on investment (ROI) can be measured.

However, building or expanding an existing SOC involves overcoming numerous complex challenges. The biggest is the difficulty of finding and retaining skilled people. SOCs can also be costly to build and maintain, a financial commitment that stretches into the future.

A fundamental issue is whether to build or expand SOCs as an internal operation or look more towards outsourced SOCs and managed services. As the market for outsourced SOC services rapidly matures, a growing number of organizations are embracing a mixture of both approaches in the search for flexibility.

Technical issues to be addressed include integrating the right suite of tools, achieving visibility on the most critical systems, managing and prioritizing alerts, and implementing automation. At the same time, SOCs must remain flexible enough to adapt to new threats and have the capacity to grow as an organization's needs evolve.

This whitepaper is an attempt to examine the most important challenges an organization faces when it embarks on a new SOC project.

What is a SOC?

Today, a typical SOC carries out a growing array of security functions:

- Prioritizing, analyzing, and responding to security alerts
- Forensic analysis of past security incidents
- Monitoring threat intelligence to detect future threats
- Generating reports for compliance purposes
- Penetration testing current capabilities on an ongoing basis
- Hiring experts with experience of handling cyberattacks
- Risk-based management such as patching and managing legacy systems

Traditional IT security is based on a reactive security model that assumes a compromise in one system can be contained and that defenders will have time to block attempts to move laterally inside networks. The rising number of reported cyberattacks has underlined the flaws in this approach: detection is weak and response too slow.

The concept of a SOC addresses these weaknesses in several ways. The biggest change is that cybersecurity becomes a dedicated department separate from the broader IT function that can view security in a unified way. Staffed with cybersecurity specialists, the SOC team's job is to monitor for threats on a 24x7 basis, speeding up alert handling, threat detection and threat response.

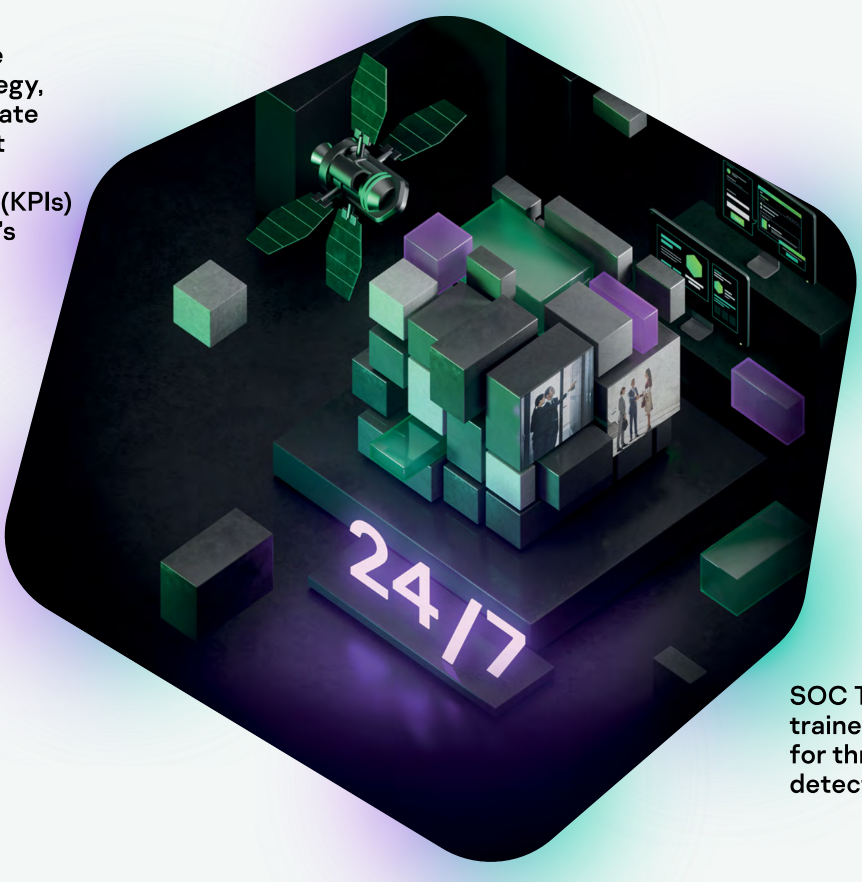
Over time, SOCs have taken on more complex tasks, such as the need to predict as well as respond to threats.

The SOC team

Building a SOC implies a logical division of labor between team members with different skills. This might include:

SOC Tier 1 – Monitoring and initial threat triage. Basically the layer of the SOC responsible for detecting threats worthy of investigation and escalating them if necessary.

SOC management – The managers who set strategy, planning, and communicate with senior management about the role and key performance indicators (KPIs) used to assess the SOC's performance.

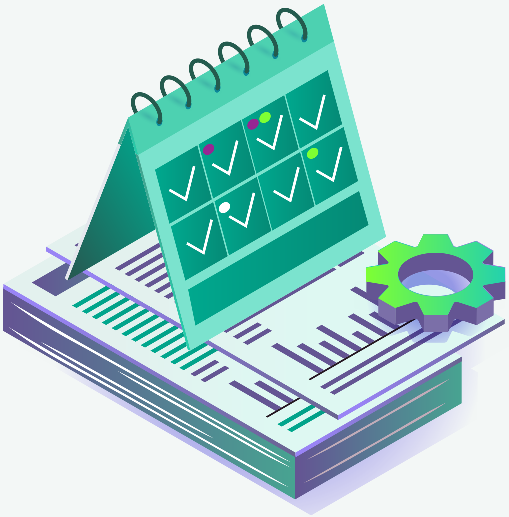


SOC Tier 2 – The investigation and response function processes these alerts, conducting deeper analysis of malware as well as forensics. Carries out isolation and remediation before feeding updates to the SIEM and threat intelligence by adding indicators of compromise (IoCs).

SOC legal and compliance experts.

SOC Tier 3 – Threat hunter trained to proactively look for threats and help tune detection.

Specialized analysts covering malware, digital forensics and threat intelligence. SOC admins – maintain and deploy SOC infrastructure and tools, validate that sensors are functioning, and that the correct infrastructure is feeding data to SIEMs. Also responsible for any custom programming required for tool automation and scripting.



SOC planning challenges

While the principle of centralizing security in a SOC is sound, putting it into practice can be a complex undertaking. Most organizations will need to develop their capability from an existing department, which might have already taken on some of the roles associated with a SOC over time. But getting this loose approach into something able to get the advantages of a full SOC capability requires experience organizations don't necessarily have to hand.

The SANS 2021 Security Operations Center survey offers insights into some of the challenges. These break down into two categories – universal problems such as hiring the right skills, and operational problems such as ensuring that the security tools and processes are up to the job. The first are the upfront problems every SOC designer knows they have, while the second manifests during or after implementation.

The never-ending skills problem

Acquiring cybersecurity skills has become an ingrained issue with no easy solution. Mentioned by 24% of SANS respondents as their biggest challenge, closing the skills gap means confronting a perennial seller's market. Organizations must not only find specific skills, but rapid changes in the skills necessary to stay up to date in this sector requires them to continuously train and retrain existing teams. The high demand for these cybersecurity skills not only makes hiring expensive but leads to the problem of retaining the best candidates. Kaspersky estimates that the average cybersecurity analyst stays with an employer for less than three years, underlining the ongoing nature of this issue.

Another hurdle is understanding which skills and experience matter in the context of a SOC as opposed to a more general IT role. These include the soft skills such as clear communication that are essential for good customer service. The assumption for anyone taking on a SOC project is that the skills shortage won't be solved easily even for organizations able to throw time and money at their SOC project.

In-house or outsourced SOC?

Despite their growing popularity, in-house SOCs remain an exception to the rule. Kaspersky's 2020 Global Corporate IT Security Risks Survey (ITSRS) of 5,266 decision makers in 31 countries found that while 52% reported having a dedicated IT security function and 14% a malware analysis team, only one in five operated an in-house SOC. Depending on sector and size this might rise to 50% in some cases, but raises the important issue of whether an in-house SOC is necessary for everyone.

Outsourced SOCs and managed security services offer a way for a wider range of organizations to gain access to the advantages of a centralized SOC without having to invest upfront. A big draw is that they solve the immediate issue of finding and hiring skilled team members. Gartner estimates that by 2025, 90% of all SOCs will have outsourced at least half their security function, increasingly as SOC-as-a-service (SOCaaS). Others will look to mix and match different elements of in-house and outsourced security.

Kaspersky's ITSRS found that 69% of respondents planned to use managed providers in the next 12 months, primarily to gain access to expertise lacking in their organization. While outsourcing to solve skills shortages might look appealing, organizations still need to assess the effect that using a third party will have on their data security and compliance state. Providers vary in their maturity level and choosing an outsourced partner for security presents challenges of its own.

Convincing reluctant boards

It's often said that management won't invest in cybersecurity until after the fact, by which time it is too late. That should make the expense involved in specifying and maintaining SOCs a non-starter and yet their popularity continues to grow. For CSOs, arguing in favor of investment involves three lines of reasoning, the first of which is that cybersecurity is best understood as being about risk assessment and mitigation. This is more likely to appeal to non-technical boards because it allows for measurable key performance indicators. A second argument is that traditional IT fragments detection and response, which requires that cybersecurity is best implemented through the centralization and scale made possible by a SOC.

A final approach is that cybersecurity is now a matter of competitive advantage. A 2019 Kaspersky survey found that organizations running internal SOCs estimated their financial hit from a cyberattack at half that of those not using one. The clear conclusion from this is that organizations investing in SOCs suffer fewer negative financial consequences over time.

Your largest outlay will be for **people** including a SOC Manager, as well as analysts, engineers, and training. People expenditure is often in the region of US$ 721,000.

For ongoing **process** costs consultancy services for use cases, playbooks, and reporting you can reckon on an approximate figure of US$200,000.

As for the **technologies** themselves, a typical cost would be around US$409,000; these include EDR, SIEM, Network IDS, Threat Intelligence, Ticketing and Monitoring, and Support.

Costing a SOC project

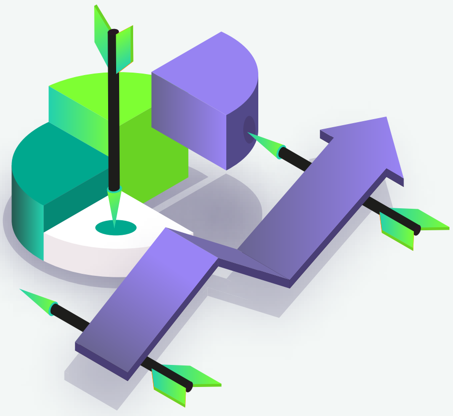
The benefits of building and running an in-house SOC are universally compelling; but the costs will naturally vary from organization to organization.

That said, ballpark figures can be enormously helpful in preparing for any strategic leap forward – and that includes building an in-house SOC. Here you can find approximate costs for the people, processes, and technologies your business will need to procure in order to derive maximum value from the revolutionary defense that only an in-house SOC can supply. All figures are given in US Dollars per annum, and apply to businesses with 1,000+ endpoints.

SOC operational challenges

Automation and orchestration

A key tension in every SOC is the need for automation, something mentioned as an issue by 23% of SANS respondents. A lack of automation risks overloading staff and consuming valuable time. Equally, cyberattacks often require the sort of automated policy actions and orchestration that can only be implemented using machine learning. Over time, this need for automation and orchestration has grown, requiring the concept to be applied in less obvious but innovative ways. SANS uses the example of an organization using automation to consolidate data fed from several divisions into a single portal. This reduced some response times by 25%. This isn't an easy demand: planning and implementing automation procedures is a complex long-term project that requires careful thought and planning.



Migration and integration of tools

The whole point of a SOC is that it provides a centralized, unified view of an organization's security state. Assembling the necessary software tools to achieve this is not always straightforward. Organizations building a SOC from scratch will have acquired their own mix of security tools across different generations, each with their own console and operational parameters. Given that SOCs are estimated to use up to 20 tools on average, this can lead to fragmentation which risks slowing detection and response. In some cases, these will need to be rationalized or reduced in number. This isn't just about having too many consoles that not everyone is trained to use. Fundamentally, these systems generate a lot of data which over time leads to the SOC equivalent of big data overload.

Too many alerts (and false positives)

A steady complaint about security systems since the invention of intrusion detection systems in the late 1990s has been the volume of alerts they generate. The addition of a new generation of applications to this via SIEM technology has only compounded the problem. More alerts risk overwhelming analysts with a high workload, reducing mean time to resolution (MTTR) or leading to alerts being ignored altogether. Furthermore, false positives generate noise, giving attackers a space to hide in and buying them time. In extreme cases this can mean that alerts are ignored altogether, reported by 3% of respondents to the SANS survey. The main reason cited was a lack of correlation between alerts generated by different systems.

Lack of enterprise and endpoint visibility

Ironically, alert overload can lead to the opposite problem of not having enough visibility of enterprise systems. Some SOCs might exclude SIEM alerts from 'noisy' systems such as endpoints that generate too many false positives. It's a fallacious version of the less is more hypothesis, an issue reported by 15% of respondents to SANS.

Endpoint detection can be complex, but limiting its scope will make the problem worse - given that these are prime targets for almost every known attack. Compromising endpoints has become so important to attackers precisely because these devices and their users are harder to lock down. This includes not only PCs and mobile devices but increasingly Internet of Things (IoT) and network devices such as printer-scanners which often have loose access control and rarely run security agents. APT attacks also increasingly probe low-level layers such as firmware, rarely monitored in real time by today's security software.

Lack of threat alert context

Even when an anomaly is detected, a lack of context can limit its usefulness for a SOC. For example, suspicious URLs are a common detection for any security system, indeed there might be thousands of these in a day. What's missing is knowing what cyberattack or malware is associated with that URL, because that gives SOCs a heads-up on what to look for in terms of possible compromise and tools,tactics and procedures (TTPs). Closing this gap requires accurate threat intelligence, which presents another blind spot. In the SANS survey, 12% of respondents mentioned a lack of threat context as their top worry.

Solving the problems

Finding the skills

Organizations wanting to attract or retain the best SOC staff often resort to raising starting salaries, which in the US have reached $125,000 for a basic analyst. While this might work initially, the frequently reported issue of high staff turnover suggests that this is not always enough to improve retention in the long run. Rising salaries across the board also risk changing the way higher-level management assesses a SOC's return on investment (ROI) which could have an impact on future investment. SOC effectiveness can be measured using different metrics, but it should not become a drain on resources.

Paradoxically, the deeper problem with SOCs could be that they become too successful in terms of work throughput. A SOC operation is always a demanding environment, which increases the possibility of staff burnout. Despite being an operational necessity, the time allocated to staff training can be reduced because of time pressures and budgetary constraints. Frequent staff turnover eventually degrades SOCs, which constantly lose staff at the point they have acquired an understanding of an organization's inner workings.

SOCs can combat these stresses by rotating staff through different roles, especially between Tiers 1-3. This not only makes working in a SOC more interesting for teams, but makes it less likely that staff at the lowest rung of the SOC, Tier 1, will outgrow their jobs after a year or two. This should be combined with a structured training program leading to certifications such as GIAC (Global Information Assurance Certification). In some companies, initial salaries are also staged to receive bonus increments after someone has been employed for one, two or three years.

Finding partners

An increasingly popular solution to the skills shortage is to outsource some SOC functions to a third party managed provider. This avoids the need to find and retain staff because these are provided as part of the service. It also removes the need to invest in regular equipment and tools upgrades, shifting cybersecurity costs from CapEx to OpEx budgets.

Smaller organizations increasingly use managed services because they lack the experience and finances to build a SOC from scratch. For medium and larger companies, assessing the balance is more complex. However, third-party SOCs and managed services don't come cheap. On top of this are issues such as managing service level agreements (SLAs) and defining how security events handled by the service provider should be escalated, mitigated and resolved.

Larger companies engage external SOCs to gain access to specific expertise or to free in-house teams for other transformation projects. It's like a pressure valve. There's also a realization that no matter how mature an inhouse SOC might be, at some point attackers will penetrate even the best defenses. When this happens, being able to call on the experience of a partner can make all the difference.

The future SOC

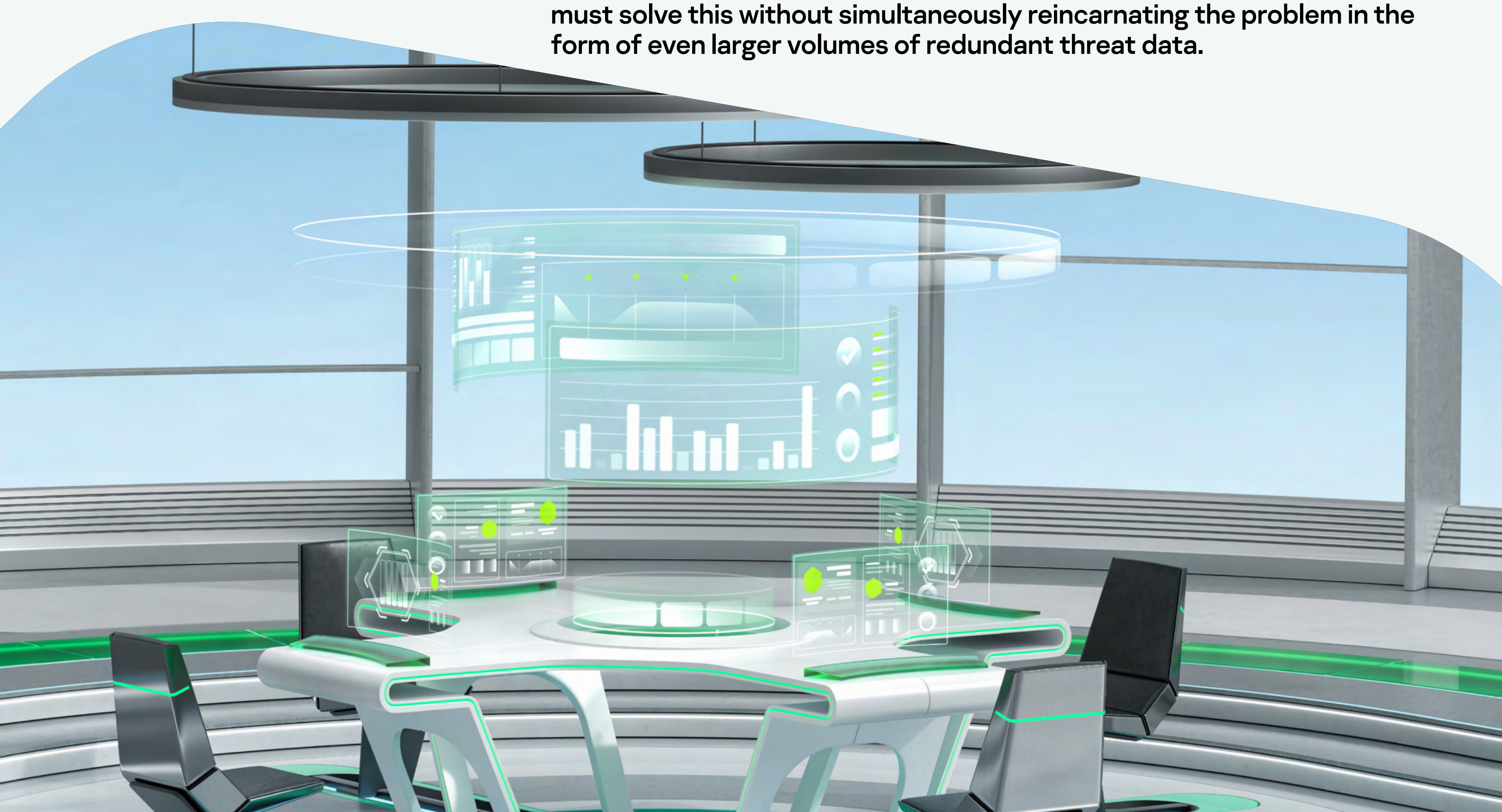
How might the rise of SOCs influence cybersecurity over the next five years?

One possibility is that as the sophistication of third-party SOC services improves, SOCaaS will become mainstream, not only for enterprises but for smaller organizations too. This will depend on the maturity of the tools offered as well as the sophistication of the services on offer. Today's security systems were primarily designed to be used by in-house IT departments although many have been adapted for SOC use. Increasingly, vendors are building a new generation of tools specifically for SOC environments. These will be optimized to cope with the SOC workflow of detecting and responding to complex threats while supporting demanding environments such as remote/home working and the cloud.

This could encourage a positive feedback loop where security systems are designed and revised more rapidly to cope with and respond to real-world detection and response rather than generalized threats. A good example of this phenomenon is ransomware which is now influencing the designs of everything from operating systems and backup systems to full-fledged incident response platforms.

Another inescapable trend is automation, an influence that is already being felt in Tier 1 threat monitoring and investigation. Increased automation is now essential for SOCs to evolve further. There will never be enough trained analysts with the time to sift through and correlate the kill chain of an attack from a morass of log data. Security providers able to provide automation tools to carry out these tasks will be at a premium.

However, the battle for the future of SOCs isn't simply about speeding up detection by giving machines more to do. SOC security processes and generates potentially huge amounts of data of its own. In theory, automation can help reduce the need for data storage by identifying which data patterns matter and which don't. Security systems are often accused of overwhelming defenders with too much data, and SOCs must solve this without simultaneously reincarnating the problem in the form of even larger volumes of redundant threat data.



How Kaspersky can help

We understand the challenges involved in building and running an in-house SOC, and we're proud of the huge advances made by our global enterprise customers in defending against APTs and similar threats by bringing the fight in-house.

With over two decades of constant threat research, leading protection technologies, recognized expertise and proven experience in complex cybersecurity projects, we can help to empower your SOC for greater efficiency at every level in fighting increasingly sophisticated cyberthreats.

Get in touch

Further recommended reading:

Managing the trend of growing IT complexity

Incident Response analyst report

Five steps to prevent IT security team burnout

www.kaspersky.com