Authors: Reinder Wolthuis, senior consultant/projectmanager cybersecurity at TNO reinder.wolthuis@tno.nl. Gert van der Lee, senior innovator/researcher cybersecurity at TNO, gert.vanderlee@tno.nl. Richard Kerkdijk, senior security consultant at TNO, richard.kerkdijk@tno.nl. Natalia Kadenko, researcher at NCSC, n.i.kadenko@minjenv.nl.

SOC of the future

Security monitoring and incident response will face major challenges in the coming years, not least because the complexity of infrastructures, threats and regulation will increase drastically. SOC managers and governmental agencies need to rethink their strategies, policies and the organization of SOCs to be prepared for these challenges. This article describes a conceptual blueprint for future SOCs that can assist the NCSC, SOC managers and CISOs in creating long term SOC roadmaps.

Cyber-attacks are developing at a rapid pace and becoming increasingly sophisticated and complex. To elevate their cyber defences, many organisations have complemented traditional (preventive) security controls with security monitoring and incident response operations. Capabilities maintained to this end are often united in a so-called Security Operations Centre (SOC). Smaller organisations that cannot maintain such provisions in-house typically outsource them to (the SOC of) a Managed Security Service Provider (MSSP). The environment, in which such SOCs operate, however, is undergoing significant changes. A prominent example is the transformation of infrastructures that SOCs are tasked to protect, which are increasingly incorporating cloud services, OT (Operational Technology) and IoT (Internet of Things) devices. Meanwhile new regulation such as NIS2, the Cyber Security Act and Cyber Shield will impose new requirements SOCs, for instance concerning their collaboration and information exchange. Security Operations Centres and government bodies such as the National Cyber Security Centre (NCSC) will need to evolve with these changes in order to stay relevant and effective.

This article presents a conceptual blueprint for the SOC by the year 2030. It reflects predicted changes in technology, organisational structures, the market for security solutions and in national and European legislation, with specific attention towards the role of government bodies at the national and European level. The article is based on a study that TNO performed in collaboration with the Dutch NCSC (SOC2030). The study consisted of literature review and interviews with various stakeholders in industry.

Current state of the SOC

Organisations can implement security monitoring, detection and response capabilities in a variety of ways and to a varying level of maturity. They usually include event - and incident management, but may also cover threat intelligence, vulnerability management and a plethora of other operational security responsibilities. These capabilities can be either maintained in-house or (partially) outsourced to service providers, such as MSSPs, and may be consolidated in one organisational entity or spread out over more. A typical example of the latter is the separation between monitoring and detection capabilities (provided by a SOC) and response capabilities (provided by a CERT or CSIRT).

The last few years have already seen a rapidly changing SOC landscape, characterized by a growing SOC-market, regulations that increasingly address security operations, a wider adoption of best practices and more, mostly sector-based, collaboration. On the whole, these developments have led to a growing overall maturity of SOCs.

Relevant developments in the coming years

Regardless of way, shape or form, the challenge for SOCs in the coming years will be - not only to monitor an increasingly complex, distributed and diverse collection of endpoints, applications and data, but - to do that facing adversaries that are constantly increasing the effectiveness of their operations through adoption of innovative technologies. On top of that, the contribution of state-sponsored actors to the threat landscape will grow significantly under the influence of geopolitical dynamics, resulting in an overall increase in complexity and impact of cyberattacks.

Technological improvements revolving around automation will enable SOCs to face that challenge and to focus more on these complex, high impact attacks. These improvements include wider adoption of SOAR solutions for security workflow automation and AI for advanced detection and analytics. And although AI's capabilities will have limitations, most experts agree that it should be able to completely replace first tier analysts by 2030.

These technological developments will also change SOC staffing requirements. They allow SOC personnel to focus more on tactical and strategic duties and on the challenges that emerging technologies and changing regulatory requirements introduce. They also allow SOC personnel to focus more on prevention, threat hunting, prediction and other proactive capabilities instead of on detection and response.

In turn, this may invite switching from a classic SOC tier-based model to a model with collaborating expert groups or cross-functional teams, consisting of threat intelligence analysts, business risk analysts, security engineers, crisis managers and data analysts. It could also trigger new core capabilities for SOCs, such as adversary emulation and impact analysis.

However, all of these developments will come at a considerable price. The cost of maintaining a proper functioning SOC will increase dramatically as a result of adopting the required technological innovations. This will force companies with in-house SOC facilities to start outsourcing some or all of their SOC capabilities to specialised service providers. It will also drive collaboration between SOCs and promote initiatives for joint SOC services in industries such as energy and water.

And finally, legislation will continue to be a driving force for cybersecurity in general and for SOC maturity in particular. IT security governance will become more mature as government institutions increase supervision and enforcement of rules and policies. Moreover, experts stress that government involvement should not be limited to legislative and supervisory roles, but should also encompass advisory work and maybe even operational assistance to essential entities and sectors.

Vision on the SOC in 2030

The blueprint for Security Operations Centres in 2030 is a thought experiment that paints a picture of the SOC-world in 2030.

Please note that the blueprint is described in a somewhat provocative form, assuming that currently foreseen trends play out to their extreme. The underlying idea is that this will likely stimulate the most valuable discussion. Also, it is conceivable that unforeseen, disruptive technologies (similar to the internet, AI and quantum computing in the past) will emerge between now and 2030 that could drastically alter the cyber landscape and consequently affect the blueprint on specific aspects.

Foreseen developments in the SOC landscape are schematically visualised in the figure below. For reference, the figure incorporates two particular variants of SOC/CSIRT instalment in an end user organisation. Here organisation A maintains in-house SOC and CSIRT operations to protect a hybrid (on-premise and cloud) technical infrastructure, whereas organisation B relies solely on cloud infrastructure and outsourced most of its security operations to a third party MSSP.

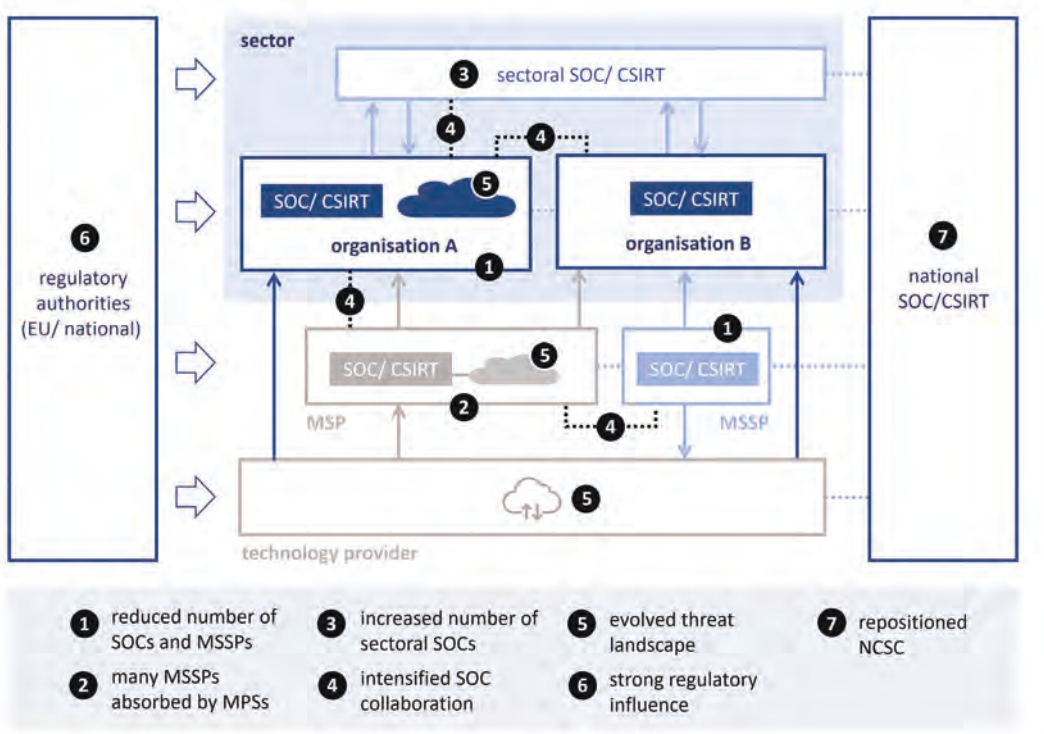

Figure 1: The SOC-landscape.

In practice, the landscape will obviously encompass a more elaborate range of deployment structures.

As shown in the figure, the authors foresee a total of 7 key changes in the SOC-landscape by the year 2030:

1. **The number of SOCs and MSSPs offering SOC services has decreased drastically.** Far fewer end-user organisations maintain their own SOC. Instead, most of them make use of the high-quality services provided by Managed Security Service Providers (MSSPs, e.g. KPN Security, Fox-IT, Pinewood) or even Managed (IT) Service Providers (MSPs, e.g. Akamai, Forescout). Consequently, the overall number of SOCs has decreased. The cost of keeping a mature SOC in operation and keeping it up-to-date is simply too high, due to the specific expertise and high degree of automation that this requires. Only a few large end-user organisations and end-user organisations that maintain specific infrastructure (such as OT infrastructure) or specific risks are able to justify an in-house SOC.
2. **MSPs have taken over much of the MSSP market.** For most of the market, the security services offered by large MSPs sufficiently fill the security monitoring needs of end-user organisations. But there will still be a role for the MSSP that has more insight in the specific context in which an end-user organisation operates. Consequently, there are new forms of collaboration between MSPs and MSSPs that offer their combined services to the end-user organisation.
3. **Every NIS3 (successor of NIS2) sector has a sectoral SOC, used for threat information exchange, and to provide collaborative monitoring, detection and response.** All the sectors to which the (fictitious) NIS3 applies have a sectoral SOC. The principal task of these sectoral SOCs is to facilitate (threat) information exchange within the sector. Many of these sectoral SOCs also offer collaborative monitoring, detection and response services to their members, although in most cases outsourced to a MSSP.
4. **A SOC and MSSP cannot operate without intense collaboration and information sharing with other stakeholders.** Information exchange between all the entities in the SOC landscape is a key element for SOCs in preventing and detecting threats. National SOCs mutually exchange information that is relevant for critical sectors and the role of

Information Sharing and Analyses Centres (ISACs) has been taken over by sectoral SOCs. Where relevant, national SOCs relay threat information to sectoral SOCs, end-user SOCs, MSSPs and MSPs within their respective countries. Besides national sharing and distribution, information is also shared bilaterally across borders, mainly by sectoral SOCs.

5. **The primary focus of SOCs and MSSPs will be on highly automated threats coming from skilled threat actors such as criminal organisations and nation states.** Threat actors at the level of script kiddies are managed in a 'business as usual' way of working and require little attention from the SOC. Attacks launched by such low-level threat actors are detected and mitigated automatically or handled as part of normal IT operations. Most attacks on end-user organisations, however, come from criminal organisations (for profit) and in some cases they are state-sponsored, (e.g. oriented at destabilizing society or stealing information). Such attacks are typically AI-assisted and mostly targeting a specific end-user organisation, which makes them hard to detect and mitigate.
6. **Most organisations make use of formally accredited SOC services, due to EU and national regulation.** NIS3 has become the essential EU regulation on cyber security. This has led to national cyber security regulations that mandate the use of SOC services for every critical sector. These SOC services need to be certified according to a defined minimum maturity level, depending on the criticality of the sector. A few widely adopted SOC maturity models drive the use of certified SOC services.
7. **The NCSC is the national SOC/CSIRT according to NIS3, the primary point for national threat information sharing and in the lead during national cyber crises.** The NCSC acts as national SOC/CSIRT (NIS3). In that role, the NCSC exchanges information that is relevant for critical sectors with other national SOCs. The NCSC has a coordinating and advisory role in the information exchange. The NCSC is in close contact with large technology providers that supply threat information. The NCSC relays relevant information to sectoral SOCs, end-user SOCs, MSSPs and MSPs where appropriate. When an incident with societal impact occurs at an end-user organisation in a critical sector or at several end-user organisations simultaneously, the NCSC coordinates the mitigating actions across all organisations involved on a national level.

In parallel to the above, the authors also foresee particular changes within the SOC and its direct environment:

The SOC focus is largely on proactive and predictive activities. Most common security incidents and vulnerabilities get detected automatically and mitigation is largely standardized and automated, for instance implemented with support of security playbooks and Security Orchestration, Automation and Response (SOAR) tools. But new and/or sophisticated attacks still require manual intervention, supported by automated (AI based) tooling for first-time incident detection and response. The focus of most SOCs is on optimizing situational awareness and predictive and proactive activities: monitoring the threat landscape and assessing threat intelligence.

Many SOC activities are automated and do not need human intervention. The detection, assessment and response to security events is highly automated with support of AI and SOAR tooling. Automation solutions have replaced first- and second tier security analysts in all but a very few (specialized) SOCs; highly sophisticated attacks also require involvement of security analysts, supported by the automated tools. The shift to cloud services offers particular potential for automated response. SOC personnel are able to focus on predictive and pro-active activities, business risk and situational awareness supported by a data lake that is filled by a multitude of internal and external data and information sources, maintained by data engineers.

Business processes such as Zero Trust decision making, benefit from the wealth of information that is available at the SOC. To do its job well, a SOC gathers an enormous amount of current information and data from all infrastructure and applications of an end-user organisation. Other business processes also profit from this information. For instance, the 'continuous decision making' (e.g. to change access rights) in Zero Trust will highly benefit from the up-to-date information sources available at the SOC.

Highly standardized technology, tooling and way-of-working enables efficient and effective performance and information exchange. SOCs and MSSPs make elaborate use of widely available standards e.g. for incident data and information exchange formats. Because of the use of these standardized formats and interfaces, the way of working is efficient and tools are interchangeable.

This paper has looked into the current state and the possible future of SOCs in the rapidly changing security landscape

Most of the infrastructure that is monitored by SOCs and MSSPs will be cloud-based. The IT-services industry has successfully transitioned to a "cloud unless" approach, leaving only classified systems, highly vulnerable intellectual property and OT as remaining on-premise infrastructure. Also 'cloud edge' solutions are broadly used. This refers to setups in which cloud technology is used on location, for example in combination with OT. This cloud focus allows SOCs to work in a highly standardized and automated way, making optimal use of the security capabilities that are built in by cloud service providers. This also makes it easier for MSSPs to standardize and automate activities across multiple customers.

A majority of SOC staff will consist of risk -, data -, threat analysts and crisis managers; only very few 'traditional' SOC analysts have remained. Virtually all traditional tier 1 and tier 2 SOC analysts' roles have disappeared, and the majority of SOC staff consists of highly skilled experts in risk analysis, CTI analysis or data analysis. These analysts operate on a tactical level and provide a new generation of core SOC services, such as collecting and processing high quality threat information, establishing situational awareness and conducting predictive analysis. With this shift to threats instead of incidents, response staff consists mostly of security engineers and crisis managers rather than traditional (security) incident responders. A challenge is to find and/or educate the few SOC analysts that are still needed, considering that the traditional career path from tier 1 to tier 2 to SOC analyst expert has disappeared.

All SOCs have abandoned the traditional tier-based SOC model in favour of flat organisational structures with staff collaborating in interdisciplinary teams. Instead of being organized in distinct tiers, SOC staff is organized in a skill- or role-based manner. This allows for a more flexible and targeted deployment of skills as cyber threats are addressed. SOCs have the mandate for making pre-emptive changes to the IT environment. A business impact threshold is agreed upon above which additional authorization (for SOC or MSSP) needs to be sought from decision makers.

Closing words

This paper has looked into the current state and the possible future of SOCs in the rapidly changing security landscape. Based on literature analysis and expert input, a number of conclusions and recommendations can be provided. First, collaboration and information-sharing will play an increasingly important role in how efficiently SOCs will be able to operate. It is therefore important to further examine the existing mechanisms and conduct research into the so far underutilized ways of collaboration. Second, most experts would encourage additional guidance and enforcement from the governmental institutions, believing that there is room for such a role. The NCSC in particular was mentioned as an institution ideally suited to play a central role in facilitating collaboration. Finally, each organization should re-examine its SOC strategy based on its needs and resources, as well as the anticipated shift from reactive to pro-active SOC.

Reference

(SOC2030) Blueprint for a Security Operations Center in 2030 – SOC of the Future, Reinder Wolthuis, Gert van der Lee, unclassified, February 27 2024, report number TNO 2023 R11803, https://publications.tno.nl/publication/34642162/x0DJXn/TNO-2023-R11803.pdf