Blueprint for a Security Operations Center in 2030

SOC of the future

TNO Publiek | ONGERUBRICEERD Releasable to the public › TNO 2023 R11803
February 27th 2024

ICT, Strategy & Policy
www.tno.nl
+31 88 86 63 741
Reinder.wolthuis@tno.nl

TNO 2023 R11803 – February 27th 2024

SOC of the future

Blueprint for a Security Operations Center in 2030

Author(s)	Reinder Wolthuis, Gert van der Lee
Classification report	TNO Publiek | ONGERUBRICEERD Releasable to the public
Title	TNO Publiek
Managementuittreksel	TNO Publiek
Summary	TNO Publiek
Report text	TNO Publiek
Number of pages	30 (excl. front and back cover and distribution list)
Number of appendices	2
Sponsor	Natalia Kadenko
Programme name	NCSC 2023 cyberweerbaarheid
Project name	SOC of the future
Project number	060.53784/01.05

Management summary

SOC of the Future

Programma		**Project**	
Programmanaam: NCSC 2023 cyberweerbaarheid		Projectnaam: SOC of the future	
Programmanummer:	060.53784	Projectnummer:	060.53784/01.05
Programmaplanning:	Startdatum 1 januari 2023 Einddatum 31 december 2023	Projectplanning:	Startdatum 15 augustus 2023 Einddatum 30 december 2023
Programmabegeleider: Jan Rooduijn NCSC		Projectbegeleider: Natalia Kadenko NCSC	
Programmaleider: Silke Mergler TNO		Projectleider: Reinder Wolthuis TNO	

Problem statement

Security monitoring and incident response will face major challenges the coming years as the complexity of infrastructures, threats and regulation increases. SOC managers and governmental agencies (such as the NCSC) need to rethink their strategies, policies and the organization of SOCs to be prepared for these challenges and to ensure an ongoing effectiveness of SOCs. Presently, there is a lack of understanding of how SOCs should evolve to address these challenges.

Project Activities

Commissioned by the NCSC, TNO completed this project to further investigate the changes SOCs will presumably undergo over the coming years. The project consisted of a literature scan and interviews with relevant stakeholders, such as SOC managers, SOC innovation partners, and other security industry representatives. The collected data was analyzed using qualitative methods to identify the main developments in SOCs up to 2030, as expected by the stakeholders. Based on the outcome of this analysis, a conceptual blueprint for future SOCs was devised and documented in this report.

Results and conclusions

This report provides an overview of the expected main developments up to 2030 and how these developments will impact the SOC. It also provides a rough sketch of the organisation, processes and interaction with the outside world deemed necessary in 2030 – a SOC blueprint. A number of recommendations for relevant stakeholders is also given.

Applicability

The blueprint can assist the NCSC, SOC managers and CISOs in revising strategies and policies, and in creating long term SOC roadmaps.

Contents

Contents

1 Introduction

1.1 Background

Cyber threats are developing at a rapid pace and are becoming increasingly complex and advanced. It is clear that preventive security measures alone are insufficient to adequately protect organisations against the impact of cyber-attacks. Many large organisations therefore complement preventive measure with detection measures and have tasked Security Operating Centres (SOCs) with monitoring their infrastructure to detect cyber-attacks. Many smaller organisations that do not have sufficient resources and budget to implement a SOC themselves outsource their security monitoring to Managed Security Service Providers (MSSPs) that perform security monitoring for them.

Currently, security monitoring and the way security monitoring is organized is undergoing significant changes.

A number of trends have been identified:

- *Progressive level of automation* – cyber-attacks are becoming more complex and the number of attacks is growing rapidly. The amount of data that is collected by the monitoring process is growing rapidly as well. To keep up with the attackers, SOCs will need to automate their monitoring and detection operations. Human operators cannot cope with the increasing complexity and number of attacks and the increasing amount of monitoring data;
- *The monitored infrastructure is rapidly changing* – The use of (public and private) cloud-based infrastructure and services, the monitoring of OT (Operational Technology) and IoT (Internet of Things) and the use of encryption in network traffic are increasing. The adoption of these new types of infrastructure (components) leads to a revised threat landscape and triggers new attack vectors. The nature of monitoring and the SOC work methods needs to be adapted to these changes;
- *Regulatory changes* – Regulatory pressure regarding cyber security coming from EU and national government is increasing (e.g. NIS2, Cyber Security Act, European Cyber Shield). These regulations also include security monitoring and incident response, as well as collaboration and information exchange between SOCs.

SOC managers and governmental agencies (such as the NCSC) need to prepare for these developments so they can determine the right strategic approach and become better prepared to deal with the upcoming challenges.

1.2 Goal

This project aims to provide insight in the developments outlined above and characterise how these developments will impact current SOCs. These insights will be accumulated into a blueprint for the SOC in 2030. The blueprint will better equip SOC managers and policy makers to future-proof SOCs. The blueprint is intended as an exercise and input for discussion rather than a set of predictions.

This report provides a rough sketch of the organisation, processes and interaction with the outside world for SOCs in 2030: a SOC blueprint. The blueprint can serve as input for strategy and policy revisions and as input for SOC managers and CISOs for long-term SOC roadmaps. Answers are given for the following research questions:

1) What are the current trends that will affect the setup and appearance of a SOC in 2030? Aspects that will be addressed include technology (e.g. AI, automation, digital twinning and modelling, DevSecOps, post-Quantum technology), the organisational structure (e.g. in-house, purchased as a service, collaboration formats) and developments in the threat landscape, SOC tooling and products and (inter) national legislation.
2) What would a mature SOC (either in-house or as a commercial MSSP) look like in 2030 with respect to for instance roles and duties, staffing, competences, scope of monitoring (IT/OT/Cloud/other), collaboration with other SOCs and relevant entities, level of automation and tools?
3) What will be the role of the national government, bodies such as the NCSC and the European Union (e.g. European Cybershield) in this future playing field?

1.3 Approach

In order to meet the goals of this project, an overview of current information on the topic was created from two main sources:

1. Literature covering academic papers, vision papers that were compiled in European R&D projects such as SOCCRATES (SOCCRATES, 2022) and white papers of vendors;
2. A number of semi-structured interviews (5-10) with relevant stakeholders, such as SOC managers, SOC innovation partners, industry and government representatives.

For the second source, questionnaires for different interviewee profiles were created and concise interview notes were made and shared with each interviewee. To ensure an ethical way of working, the applicable internal data management protocol was followed. Each interviewee provided consent and was made aware that their participation was voluntary and that consent could be withdrawn at any time. As requested by the interviewees, no pseudonymization has taken place; the names can be found in Appendix A.

The information gathered in the steps above was analysed in a qualitative manner to extract the main developments for the SOC up to 2030. Based on these developments and knowledge gained, a draft SOC 2030 blueprint was created. These draft results were offered for review to a number of relevant stakeholders, with the review comments included in the final version of the report. The ambition is to also publish the results in collaboration with the NCSC (as a non-specialist paper) and to present the results at relevant events.

The target audience for this report are:

- The NCSC;
- Policy makers on different levels;
- SOC managers;
- SOC analysts;
- Chief Information Security Officers (CISOs).

1.4 Reader's guide

Chapter two describes current SOCs and provides a working definition of a SOC for the purpose of this report. Chapter three describes the relevant SOC developments expected between 2024 and 2030, based on the findings from the literature scan and interviews. Chapter four translates these SOC developments into a blueprint for SOCs in 2030. Chapter five lists some recommendations.

2 Current state of the SOC

2.1 SOC, CSIRT and MSSP

Traditionally, cyber security was mainly focused on the implementation of preventive measures: 'building a wall' around the infrastructure to protect it from cyber-attacks. But in the last decades, the cyber threat landscape has greatly evolved, the threat actors have changed and the infrastructure that needs to be protected has changed as well. Preventive measures alone did not suffice anymore for adequate cyber security and cyber resilience; they needed to be complemented with detection and response capabilities, as well as pro-active measures such as sharing CTI, threat hunting and threat landscaping. This report focusses on the detection and response capabilities; especially the developments in the coming 7-10 years. But to do that, we first need to picture the current state of affairs in this field.

Many organisations have setup internal SOCs and CSIRTs to implement detection and response capabilities, others outsourced (some or all of) these capabilities to an MSSP.

Both a SOC and a CSIRT[1] are expert teams that provide operational security services to an organisation. They can either be organized informally as (virtual) teams or be embedded in the organisational structure as formal departments. The definition of the tasks that a 'SOC' and a 'CSIRT' need to perform is rather context dependent; not all organisations assign the exact same set of tasks to these two teams. To complicate things even more, different names are used, such as 'Cyber Defence Centre', which might combine both SOC and CSIRT functions. Frequently, a SOC is largely focused on monitoring and detection, in many cases organized in a two-tier model with two levels of analysts: first line (initial triage) and second line (detailed analysis and response of incidents with simple and well-known response). Response and mitigation of detected security incidents that are complex, unknown or require elevated mandate for response ('escalated response'), is then handed over to the CSIRT. The CSIRT mainly coordinates the mitigation actions that usually need to be implemented by other parts of the organisation (e.g. the infrastructure maintenance engineers).

Some organisations may choose to outsource (part of) their SOC or occasionally even CSIRT tasks to an MSSP, for instance because they may not have the expertise nor the resources to build and maintain their own in-house SOC (or CSIRT) capability. Resources are even more an issue when they require 24/7 security monitoring and response operations. The MSSP usually performs (24/7) monitoring and detection services for the organisation and informs the organisation when security incidents are detected, so the organisation can start incident response. If an organization has setup a CSIRT, then the CSIRT will generally be the point of contact for the MSSP.

[1] CSIRTs are known under several different names. Another common name is Computer Emergency Response Team (CERT).

An increasingly important task for incident monitoring, detection and response is the use, creation and exchange of Cyber Threat Intelligence (CTI). Mature SOCs and MSSPs generate their own CTI and also collect CTI from different sources (e.g. commercially purchased, distributed by government, received from vendors). CTI becomes more powerful when it is shared with others. The purpose of sharing is on the one hand to have reliable CTI from trusted sources and on the other hand to collaboratively enhance the meaning and context of CTI, so sharing adds value for each sharing partner. Sharing CTI is often done in communities. A community can be e.g. organisations in one sector or the EU member states. When a community is built up of organisations in one sector, sector-specific communities have been created, called ISACs (Information Sharing and Analysis Centres). For most critical sectors in the Netherlands, ISAC's are available; NCSC facilitates ISACs as sharing platform. But participation for organisations in an ISAC is not mandatory. ISACs gather, analyse, share, and coordinate information about cyber threats and incidents among critical infrastructures or industry sector entities (e.g., the finance sector). ISACs can also facilitate data sharing among public and private sector groups in accordance with government policies or national laws and might even be organized as public-private partnerships[2]. ISACs are founded to share information on a tactical level (e.g. development in threats and threat actors). But there also was a growing need to share operational information. SOCs and CSIRTs - depending on where this sharing activity is implemented - started sharing this operational threat information (e.g. Indicators of Compromise) with other SOCs/CSIRTs, either in the same sector or cross-sector. The following picture (SOCCRATES, 2022) depicts the SOC and CSIRT clustering and layering as currently is ongoing. There is a collaboration of nations within the EU, collaboration on national level with sectoral CSIRTs and companies and MSSPs, and also collaboration within specific sectors.

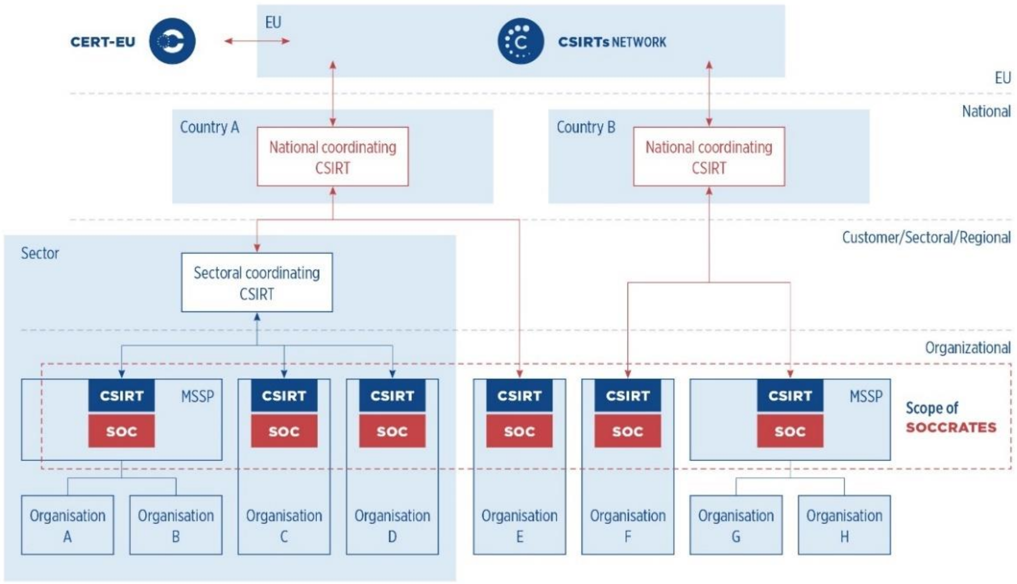


Figure 1: SOC and CSIRT clustering and layering (source: SOCCRATES vision paper)

[2] https://www.first.org/standards/frameworks/csirts/team-type

Currently, the SOC/CSIRT landscape is changing rapidly and the overall maturity is growing. The following is a non-exhaustive summary of the current state of affairs for some of the areas that undergo change.

- SOC and CSIRT are becoming more closely intertwined – as mentioned above, there is not a really strict separation anymore between the activities of a SOC and CSIRT. Sharing of threat intelligence can be done by both, a SOC could handle part of the incident response and also perform activities that can be seen as typical CSIRT activities (such as threat hunting).
- Sectoral CSIRTs are gaining importance – We see an increasing number of sectoral CSIRTs in the EU. One reason is that it is easy to collaborate with organisations that have comparable processes and issues. In the Netherlands, these sectoral CSIRTs also emerged because the focus of the Dutch NCSC mainly was on the critical sectors. Some sectors that were not tagged as critical sector then formed a sectoral CSIRT, to jointly counter the cyber security challenges. At this moment there are 6 sectoral CSIRTS in the Netherlands (Oldengarm, 2023):
    1. The National Cyber Security Center for the National Government and critical sectors (NCSC)
    2. The CSIRT for digital services (CSIRT-DSP)
    3. CERT Water management (CERT-WM) for the regional water authorities
    4. Information Security Service (IBD) for the Dutch municipalities
    5. The CSIRT of SURF (SURF-CERT) for knowledge institutes and education
    6. Z-CERT, the sectoral CSIRT for healthcare

  Two of these (SURF-CERT and Z-CERT) have also included (or plan to include) collaborative outsourcing of SOC monitoring services as a shared service for their sector.
- EU regulations increasingly addresses security operations – Several new regulations from the EU that include SOC/CSIRT type of activities have been or are being introduced. This includes NIS2 (obligation for monitoring and response activities) and European Cybershield (obligation to create 'national SOCs').
- Increasing availability of standards and best practices – A lot of efforts are ongoing to publish best practices how to design SOC and CSIRT processes and standardize the technology used in SOCs and CSIRTs. These are mainly industry initiatives and examples include the FIRST Services Framework (FIRST, 2019), MITRE's '11 strategies of a World-Class Security Operations Center' (Kathryn Knerler, 2022) and OASIS Open[3].
- Advent of SOC and CSIRT Maturity models – With the growing maturity of SOCs, there was a need to measure the maturity of SOC and CSIRT capabilities and consequently to set a target for the desired SOC maturity. One of the widely used models for this is the SOC-Capability Maturity Model, SOC-CMM[4]. The maturity of a CSIRT can be measured and even certified according to Security Incident Management Maturity Model, also called SIM3[5].

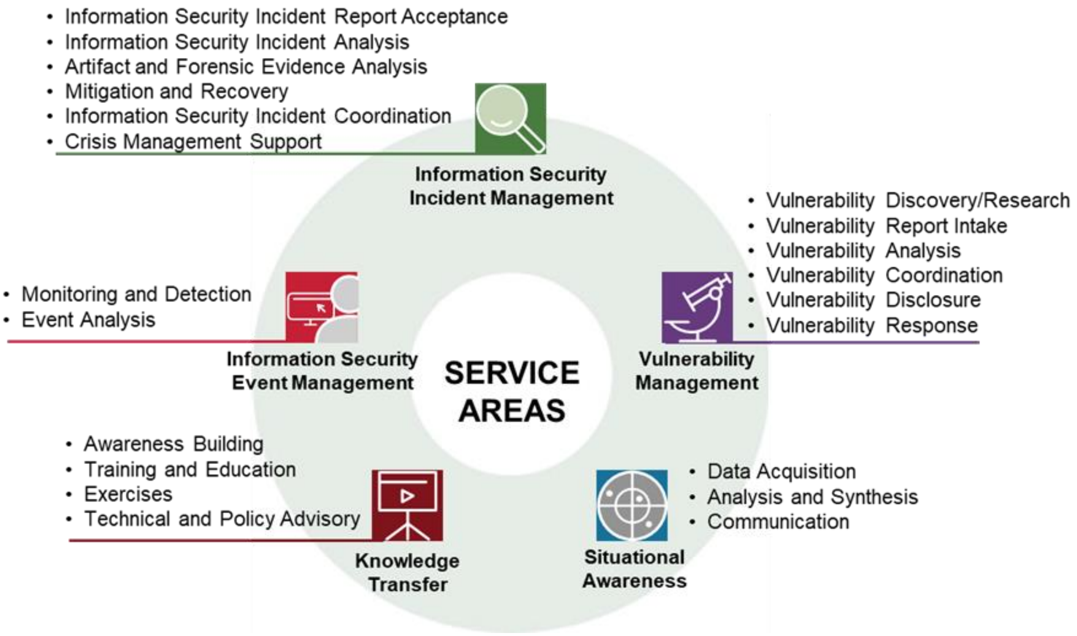
2.2 SOC scope

In this report, an assessment is given of the SOC developments over the coming years, which have led to a conceptual design for SOCs in 2030. As a starting point, a working definition of the current SOC was developed. In practice, both at end-user organisations with their own SOC and at MSSPs in their service portfolios, various terms are used to label security monitoring and response activities, for instance, Cyber Defence Centre, SOC, CSIRT,

[3] https://www.oasis-open.org/
[4] https://www.soc-cmm.com/
[5] https://opencsirt.org/csirt-maturity/sim3-and-references/

CERT. It is not always clear what tasks, duties or services are included in such labels. In ENISA's *"How to setup up CSIRT and SOC"*, (Edgars Taurins, 2020), a set of services has been identified that are typically provided by a SOC and CSIRT. These services are a subset of the CSIRT services framework compiled by the Forum of Incident Response and Security Teams (FIRST) (FIRST, 2019). Another good reference for categorizing SOC and CSIRT services is the report by MITRE describing the '11 strategies of a world class SOC' (Kathryn Knerler, 2022)

For the purpose of this report, we will define a SOC according to the Services as listed in the report of FIRST (FIRST, 2019): Team Types Within the Context of Services Frameworks[6] an addendum to the CSIRT services framework of FIRST - see also Figure 2. In light of the intertwined functions of SOCs and CSIRTs, this report uses a rather broad definition of SOC that includes some of the services that are traditionally considered to be CSIRT services.



• Information Security Incident Report Acceptance
• Information Security Incident Analysis
• Artifact and Forensic Evidence Analysis
• Mitigation and Recovery
• Information Security Incident Coordination
• Crisis Management Support
Information Security Incident Management
• Vulnerability Discovery/Research
• Vulnerability Report Intake
• Vulnerability Analysis
• Vulnerability Coordination
• Vulnerability Disclosure
• Vulnerability Response
Vulnerability Management
• Monitoring and Detection
• Event Analysis
Information Security Event Management
SERVICE AREAS
• Awareness Building
• Training and Education
• Exercises
• Technical and Policy Advisory
Knowledge Transfer
• Data Acquisition
• Analysis and Synthesis
• Communication
Situational Awareness

Figure 2: The five Service Areas and Their Associated Services of the CSIRT Services Framework v2.1 (source: (FIRST, 2019))

The selection is based on the services that most MSSPs offer as SOC/CSIRT services and most end-user organisations include in their SOC/CSIRT organisation (and/or acquire from MSSPs). The selection includes the minimal SOC and CSIRT services as indicated by the ENISA report (Edgars Taurins, 2020).

Working definition of SOC for the purpose of this report
A SOC provides at least the following services:

- Information Security Event Management
  - Monitoring and Detection
  - Event Analysis
- Information Security Incident Management
  - Information security incident report acceptance
  - Information security incident analysis

[6] https://www.first.org/standards/frameworks/csirts/team-type

  - Information security coordination
  - Mitigation and recovery
- Vulnerability management
  - Vulnerability discovery / research
  - Vulnerability analysis
  - Vulnerability coordination
  - Vulnerability response
- Situational Awareness
  - Data acquisition
  - Analysis and synthesis
  - Communication

From Knerler (2022) we can add the following SOC Functional Categories:

- Cyber Threat Intelligence, Hunting, and Analytics
- SOC Tools, Architecture, and Engineering. ((Kathryn Knerler, 2022), page 14-15)

3 Relevant developments between 2024-2030

This chapter describes the relevant developments in the SOC and CSIRT field on the basis of eight different aspects. The chapter combines input from literature with input from interviews.

3.1 SOC landscape

Organisations have several deployment options when it comes to SOCs. As depicted in figure 1, SOCs can be deployed inhouse or partly or completely outsourced to an MSSP (SOCCRATES, 2022). The 'SOC landscape' depicts the ratio between these deployment types, the types of services that are on offer through MSSPs and the collaboration between these (different types of) SOCs. Based on current and foreseeable trends and developments, the consensus among interviewed experts (see Appendix A) is as follows.

In the next few years, inhouse SOCs will remain the better option for large businesses and government. This is equally true for organisations that have specific (on premise) infrastructure, such as telecom 5G and electricity OT infrastructure. The SOC success, however, will depend on their ability to sustain both suitable personnel and proper funding, as adopting required technological innovations will put a strain on both. Not being able to keep up with these developments may force organisations to turn to the services of MSSPs.

At the same time, a shift in the SOC market may occur where medium-sized organisations no longer purchase SOC services from MSSPs. Instead, they will opt for adding SOC services to existing generic IT-services from large vendors (such as Microsoft) as an additional licensed feature. This shift is enabled by the increasing availability and use of cloud services (SaaS, PaaS). Cost saving and these vendors' unrivalled ability to execute will be the main considerations in this case.

Together, these developments will reshape the MSSP SOC-market, although it remains to be seen how exactly. While some experts foresee a strongly diminishing MSSP SOC-market in the next couple of years (because the MSSP SOC services will be included in MSP services), others expect it to thrive because knowing the customer context is very important. Some experts expect a merger of MSSPs and MSPs, alongside a more fundamental shift in focus away from detection and response and more towards secure design and pro-active measures such as threat landscaping.

For small organisations, purchasing a SOC service as part of a generic IT-service package from a large vendor becomes a viable option, as other options are generally too expensive. The lack of transparency for these services, however, may become a concern, as the same entity would then be responsible for both offering the infrastructure and monitoring it.

Inter-SOC collaboration becomes key in the coming years, especially concerning the exchange and collaborative generation (using e.g. deception technology) of Threat Intelligence. Situational awareness will become one of the fundamental pillars for an effective SOC, more so than it is today. And the availability of actionable and vetted, organisation-specific Threat Intelligence is a core necessity to achieve that. This makes it essential for SOCs to work together in this area.

Although collaboration between MSSPs will remain difficult because of conflicting commercial interests, collaboration between companies in the same sector could thrive. Current examples of successful collaboration in SOC services and/or Threat Intelligence exchange include Academic- (SURF), Healthcare- (Z-CERT) and Local Government (GGI-Veilig) sectors. It is not difficult to visualize a similarly successful collaboration for sectors such as Energy, Water, Food industry, Research and Production.

Another form of collaboration that is expected to take further shape in the coming years is international collaboration. These could be either industry-driven initiatives, such as the European ISACs, or government-driven initiatives, such as cross-border SOC platforms, as mentioned in (European Commission, 2020).

3.2 SOC technology

One of the collective viewpoints of interviewed experts is that, at the moment, there is a lot of room for improvement in SOC effectiveness through automation of SOC tasks. Not only through the use of Security Orchestration, Automation and Response (SOAR) or Endpoint Detection and Response (EDR) solutions, but also through more traditional forms of automation, such as scripting. As mentioned in (SOCCRATES, 2022), deploying SOAR capabilities has its challenges, such as the diversity of security products and tools that need to be integrated and the amount of tuning that is required. However, the benefits of increased effectiveness will become invaluable in the following years, when the number and complexity of threats requiring attention from SOC staffing continues to grow.

Examples of automated SOC tasks that could emerge in the coming years include:

- Pre-filtering events for analysis through AI and enhanced software tooling
- Calculation and suggestion of Courses of Action through AI
- Collecting relevant information and context to assist in event analysis through enhanced software tooling
- Simulation of the impact of security events through the use of infrastructure models and digital twins
- Better detection capability through the use of infrastructure models and digital twins

AI will also play a part in the SOC automation process over the next couple of years, but its capabilities will have limitations and it is unclear in how far AI will be capable to take over manual SOC tasks. Some context on the use of AI is provided in a blogpost by Rob van Os (Van Os, The AI driven SOC: a glimpse into the future of security operations, 2023). The application of AI in automation of certain SOC tasks, such as event detection, has some challenges. One of the challenges is the explain ability. When AI is used to automate SOC tasks, are we then able to explain whether the most optimal mitigation strategies were applied? Another major challenge is the lack of high quality training data. This is caused by low willingness among organisations to share sensitive data on real world cyberattacks. In spite of this challenge, most experts agree that AI will be able to completely automate first tier analysts, probably by 2030. Some will even go as far as to say AI will almost completely replace all operational level SOC personnel, including tier 2 analysts. Others, however, warn of expectations for AI being too high, as AI is fundamentally different than human intelligence.

Together, these are the first steps towards a more autonomous cyber security posture for the future, a glimpse of which is offered by the TNO position paper “Checkmate, cyber security?” (TNO, 2023) and Google Cloud’s Autonomic Security Operations (Iman Ghanizada, 2021) .

In general, experts agree that quantum computing will not play a major role in 2030 just yet. However, as we’ve seen with the surge of generative AI in 2023, the emergence of breakthrough technologies can drastically alter the cyber landscape. A time frame of seven years surely allows for the emergence of such a disruptive technology in some way or form, whether it concerns AI, quantum technology or something entirely unthought of as of today.

In (Johnson & Awuah, 2021), some other technical developments that potentially find their way to the SOC are mentioned, such as Artificial neural networks (ANN) that can be trained to discover hidden CTI patterns in data without the involvement of specific human knowledge to make predictions and deep reinforcement learning (DRL) to solve complex and sophisticated intrusion detection problems.

3.3 Infrastructure under monitoring

Recent years have seen an increase in complexity, distribution, diversity and dynamics of endpoints, applications and data. The abundance of mobile devices, the continued migration of services to cloud-based infrastructure and the ease with which new applications can be purchased and introduced are just a few examples of this development. The modern IT landscape for any organisation today is a mix of on-premise and cloud-based infrastructure, providing a plethora of applications to employees and customers.

This trend is expected by most experts to continue over the next couple of years. From a security perspective, this requires a holistic approach where the focus of both proactive and reactive security measures, including those provided by SOCs, shifts further away from the network and more towards the data layer. Where experts disagree, is if and how this can be achieved. Suggestions include wide adoption of Zero Trust architectures, using AI for application- and user behaviour monitoring and global standardization of APIs and data access monitoring functions. But what is mentioned most, is the ability of cloud infrastructure providers to offer appropriate security monitoring capabilities to their service offering.

The move to cloud infrastructure also introduces more potential for automated response in the infrastructure. Cloud infrastructure in essence is built with virtual computing technology (such as Network Function Virtualization and Software Defined Networking), which can be easily controlled in an automated way thus enabling automatic implementation of response measures.

One type of system that will remain (partly) exempt from the trend of migrating to cloud-based infrastructure is Operational Technology (OT). As the recognition of the importance of proper security monitoring for OT-environments has increased, SOCs are starting to close the gap between their IT- and OT-monitoring capabilities. This effort will continue over the next couple of years and may remain a focus point for SOCs for many years to come, given the ever increasing trend of making things “smart”.

3.4 Staffing

We see a growing shortage of skilled cyber security personnel, that will impact the staffing of SOCs and CSRITs (Jansen-Ferdinandus, 2018), (SOCCRATES, 2022). One way to deal with this is prioritization of services that a SOC/CSIRT offers (Jansen-Ferdinandus, 2018). Another way to deal with the issue of staff shortage is automation. As mentioned earlier, SOC technology developments will enable automation of operational SOC tasks, especially repetitive first tier tasks, which might relieve the pressure on staffing. Experts are unanimous in their opinion that automation will change SOC staffing requirements and cause a decline in the need for classic first tier analysts. In (Johnson & Awuah, 2021) this is described as moving from Human in the Loop (HITL) to Human on the Loop (HOTL), that allows the automation to autonomously perform a task whilst the SOC analyst monitors and intervenes the operations only when necessary.

This development also allows SOC personnel to focus more on the tactical and strategic levels, as mentioned in the “Project 2030” Whitepaper by security vendor Trend Micro (Baines, 2021), or on the challenges that emerging technologies and changing regulatory requirements introduce, as mentioned in the (ISC)^2 Cybersecurity Workforce Study 2022 ((ISC)2, 2022). It also allows SOC personnel to focus more on prevention, threat hunting and prediction instead of detection and response, which may result in SOCs focusing more and more on proactive capabilities.

All of these developments may invite switching from a classic SOC tier-based model to a model with collaborating expert groups, such as:

- Threat Intelligence analysts, responsible for Situational Awareness and predictive analysis
- Business / Risk analysts, responsible for assessing risk from a business resilience perspective and deciding on Course of Action
- Security engineers, responsible for anticipating predicted threats and optimizing infrastructure security
- Crisis managers, responsible to coordinate the mitigation of large cyber incidents

A similar model, but with different subject matter experts is suggested in the whitepaper “Future of the SOC: Skills Before Tiers” by Deloitte and Google Cloud (Deloitte, GoogleCloud, 2020). The LinkedIn post of Rob van Os (Van Os, No more Tiers, 2023) confirms that SOC operations will develop towards a tier-less model.

Furthermore, as SOCs become more data driven and technology assisted, there will be an increase in SOCs deploying generic data scientists, -engineers and -analysts.

Although the exact composition of SOC staff remains unsure, it seems inevitable that it will be more diverse in terms of skills and roles than it is today.

A downside of automation of basic SOC tasks, such as event analysis, is that it may put even more strain on the availability of personnel with the required technical skills to provide in-depth analysis of cyber-attacks. When SOC staff not regularly conducts in-depth technical assessments of security incidents, the technical knowledge and skills to conduct these assessments will slowly disappear; when really new incidents appear that automated tasks cannot solve, humans will also no longer be able to solve these. So we need to be aware that these technical skills are still available.

3.5 Internal organisation, processes, mandate

Developments described in the previous sections will also change the way SOCs are organized, as can be seen from the following examples.

Situational Awareness was mentioned as a key pillar for an effective SOC of the future. This means gathering high-quality, organisation-specific Threat Intelligence, required to uphold proper Situational Awareness will become a more important and elaborate process than it is today. By definition, Situational Awareness is context sensitive, so it is up to the individual organisations to create it for their own context. The information gathering to create Situational Awareness requires better internal information sources and more collaboration with external entities, such as other SOCs.

Acting on this information in a proactive manner requires the involvement of Risk Analysts and close alignment with the business, as well as Security Engineers to implement necessary countermeasures. This would then require broadening the SOC mandate to not only commission necessary changes to the IT environment (through IT operations) during incidents but to have the authority to automatically implement changes in the infrastructure and also to commission preventive measures.

Furthermore, the collaboration of these different types of roles is better organized through expert groups or cross-functional teams, instead of classic tier-based SOC structures. It could also trigger new core capabilities for SOCs, such as adversary emulation and impact analysis, leading to even more new processes and workflows.

Experts acknowledge there is a lot of uncertainty in how the organisation of SOCs will change, given the aforementioned developments. However, SOC teams that have already put aside the tier-based model and adopted an agile mindset to deal with the dynamics of the years to come do seem to have an advantage.

3.6 Threat landscape

In (ENISA, 2023), ENISA identifies emerging cybersecurity threats, some of which would be relevant for SOCs:

- Supply chain compromise of software dependencies
- Human error and exploited legacy systems within cyber-physical ecosystems
- Targeted attacks (e.g. ransomware) enhanced by smart device data
- Exploitation of unpatched and out-of-date systems within the overwhelmed cross-sector tech ecosystem
- AI disrupting / enhancing cyber attacks

Although these specific threats offer some insight in things to come, they do not seem to reflect any underlying trends. Interestingly, interviewed experts did mention trends rather than specific examples of future threats.

As has been the trend for a long time, our increasing dependency on digital services and a continuing trend of making things “smart”, makes society increasingly more vulnerable to cyber-attacks. It increases not only the attack surface for threat actors, but also the potential impact of cyber incidents on our daily lives.

Cybercriminals are expected to remain a major contributor to cyber-attacks in the coming years. As one expert put it: there is money to be made and they will not leave it on the table. Extortion of victims will remain their number one business model, using ransomware, data theft and denial of service tactics as they have been in recent years.

The contribution of state sponsored actors to the threat landscape will grow significantly under the influence of geopolitical dynamics. The war in Ukraine is an excellent example of the role that state backed cyber actors may have in times of international tensions. The most apparent example is the massive cyber attack that damaged the IT infrastructure of Ukraine's biggest mobile operator Kyivstar. Services of the company, which counts more than half of Ukraine's population as mobile subscribers, were knocked out after hackers used an employee's compromised account to carry out the attack. A group called Solntsepyok, (allegedly affiliated with Russian military intelligence), claimed responsibility for the attack. Earlier examples would be the 2016 and 2020 American presidential election interference attempts.

Threat actors are expected to increasingly use AI and Large Language Models (LLMs) to increase the effectiveness of their operations, see e.g. (Bussier, 2023), (Erzberger, 2023), (Paganini, 2023). Examples include AI-assisted search for zero days and coding of malware. This also allows for a further “industrialization” of cybercrime.

Where the expert opinions diverge, is when it comes to specific examples. One expert expects a shift in attacker focus from exploiting user vulnerabilities (clicking on a malicious link) to exploiting software- and hardware vulnerabilities. Another specifically mentions an increase in insider threats. Others expect attackers to “keep it simple” and stick to one of the cheapest and most effective weapons of choice today: guessed and stolen credentials.

3.7 Standardization

It is hard to identify relevant developments on the subject of standardization. Although standardization is a valued process in cybersecurity in general and SOCs specifically, there is hardly any literature available describing trends and developments regarding the subject. Moreover, the subject was only specifically mentioned three times during the interviews with experts.

Standardization and certification could allow MSSPs to distinguish themselves in the future SOC market. Standardization and certification are likely to be increasingly used tools for governments to enforce proper Security Monitoring in light of recent legislation. And standardization could play a role in the increasingly important exchange of Threat Intelligence between SOCs in the future.

3.8 Role of government and regulations

Interestingly, as can also be seen from some of the phrasing in this section, when the subject of government comes up, experts deviate from stating their opinions and expectations for the future to expressing their wishes and preferences concerning government involvement.

Nonetheless, legislation is expected to continue to be a driving force for cybersecurity in general and SOC quality in particular. IT security governance becomes more mature as government institutions increase supervision and enforcement of rules and policies. In that sense, legislation supports security specialist in reaching their goals.

However, multiple experts stress that government involvement should not be limited to legislative and supervisory roles, but should also encompass advice, mediation and maybe even operational assistance to essential entities and sectors.

Stimulating collaboration, especially where it concerns the exchange of Threat intelligence and enabling and supporting sectoral SOC- and CERT-initiatives, is also seen as a key role for government institutions in the coming years.

And finally, several experts specifically mention limiting factors concerning government involvement in the coming years, such as uncertainty about the mandate of government institutions and their perceived inability to recognize technological trends and set the rules of engagement for those trends in a timely manner.

4 Vision on the SOC in 2030

4.1 SOC Blueprint 2030

This section describes a blueprint for Security Operations Centres in 2030. This blueprint is a thought experiment that paints a picture of the SOC-world in 2030 given the trends and developments outlined in the previous chapter. The blueprint addresses what all major topics that are relevant for SOCs could look like in 2030. To create awareness and stimulate discussion, the topics will be described in a somewhat provocative but realistic way, according to the extreme variants of the trends in chapter 3.

One caveat that needs to be mentioned is that between now and 2030 currently unforeseen, disruptive technologies (such as we have seen in the past with for instance the Internet, AI, Quantum computing) could emerge. These could drastically alter the cyber landscape and consequently could make the blueprint as described in this chapter inaccurate on specific points. Furthermore, the reader is encouraged to consider this chapter as an exercise and input for discussion rather than a set of predictions.

4.2 Rationalized Landscape

For the sake of the blueprint, we have formulated the following definitions:

- **Technology provider**: a tech firm that develops and offers IT infrastructure technology as a service. Examples are Microsoft, Google, Amazon, Cisco.
- **Security vendor**: a company that offers dedicated security products and solutions. Examples are Fortinet, Palo Alto, SentinelOne, Imperva.
- **Managed Service Provider (MSP)**: Service provider that offers IT services to its customers. Often these services make use of the technology that is offered by **technology providers**. Examples are Perium, Akamai, Forescout.
- **Managed Security Service Provider (MSSP)**[7]: Service Provider that offers security services to their customers. Often these services make use of the security technology of security vendors and apply it to the security of IT infrastructure that is offered by MSPs and Technology Providers. Examples are KPN Security, Fox-IT, Pinewood.
- **End-user**: company or (government) organisation that has its own SOC or that makes use of the services offered by MSPs and MSSPs but also uses tools and products that are offered by Technology providers and Security vendors. Examples are ABN AMRO, KPN, ING, ASML.
- **NIS3:** the follow-up of NIS2 and published in 2028. NIS3 is a fictious standard, introduced in this report for the sake of discussion. It is more detailed and more widely scoped than NIS2.

Figure 3 below depicts the Rationalized SOC landscape of the Blueprint. The paragraphs following the picture describe the different topics that in the SOC landscape of the future. They are depicted in the red text in the picture.

[7] In many cases, security companies offer both security services and security products, thus combining the roles of MSSP and security vendor

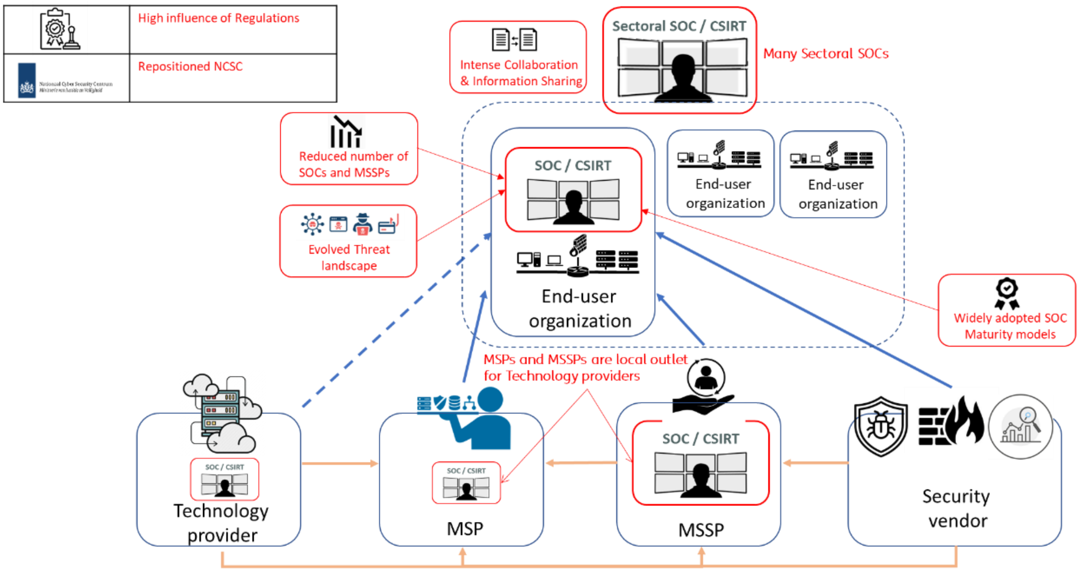


Figure 3: Rationalized SOC landscape of the Blueprint

4.2.1 Reduced number of SOCs and MSSPs

The number of SOCs and MSSPs offering SOC services has decreased drastically.

Far fewer end-users will maintain their own SOC, and consequently the number of SOCs will have decreased. In 2030, the cost of keeping a mature SOC in operation and transforming it to keep up with all developments is simply too high due to the specific expertise that is needed to manage the SOC processes and the required high degree of automation. In addition, the quality of SOC services offered by MSSPs will at least equal the quality of an in-house SOC and often even exceed it. Only a few large end-users and end-users that have specific infrastructure (such as OT infrastructure) or specific risks (highly critical or confidential information) are able to justify an in-house SOC. All other end-users have chosen to outsource their SOC services to MSSPs, MSPs or Technology providers or jointly make use of a sectoral SOC (see par. 4.2.3).

4.2.2 MSPs and MSSPs are local outlet for Technology providers

MSPs have taken over much of the MSSP market.

For most of the market, the security services offered by large MSPs will suffice for the security monitoring needs of End-users. A fictious future service could for instance be SMART (Security Monitoring and Automatic Response to Threats), available as an add-on license to MSP products. But there will still be a role for the MSSP, that has more insight in the specific context in which an End-user operates. Consequently there are new collaborations between MSPs and MSSPs that offer their combined services to the End-user. In this case, the MSSP specializes in the security of the infrastructure services offered by the MSP. The MSP unburdens the End-user for their infrastructure services and the MSSP unburdens the End-user in their SOC and security needs.

4.2.3 Many Sectoral SOCs

Every NIS3 sector has a sectoral SOC, used for threat information exchange, most of the sectoral SOCs also provide collaborative monitoring, detection and response.

All the sectors as described in the (fictious) NIS3 will have a national sectoral SOC. The principal task of these SOCs is information exchange within the sector. The sectoral SOC ensures mutual exchange of Cyber Threat Information but also distributes CTI from other sources to its members. Also, a sector relevant threat landscape is maintained. A majority of these sectoral SOCs also offers collaborative monitoring, detection and response services to their members. These services in most cases are outsourced to a MSSP, in some cases the sectoral SOC implements their own monitoring, detection and response services.

4.2.4 High level of collaboration & information sharing

A SOC and MSSP cannot operate without intense collaboration and information sharing with other SOCs/MSSPs, government and technology providers.

Information exchange between all the entities in the SOC landscape is a key element for SOCs in preventing and detecting threats. On a national level, the national SOCs exchange information that is relevant for critical sectors with other national SOCs. The large technology providers also provide input for this exchange. The role of ISACs has been taken over by sectoral SOCs. Where relevant, information gets distributed within a country by the national SOC to sectoral SOCs, End-user SOCs, MSSPs and MSPs. The other way around, sectoral SOCs, End-user SOCs, MSSPs and MSPs share relevant information with their national SOC. One example is the sharing of ‘sightings’. A sighting is a detection on a system or network of an indicator that was received as threat intel information. This is very relevant for other organisations because an indicator that was spotted on one network has a high probability to also appear on another network. Sightings usually include sensitive information and therefore sharing this information is complicated. But with the introduction of techniques that enable sharing while guaranteeing anonymity and confidentiality (such as Multi Party Computation), these hurdles were overcome. Besides national sharing and distribution, information is also shared bilaterally across borders; this is mainly done by national sectoral SOCs. Information exchange is a topic of mutual benefit and is partly regulated; the role of commercial threat information providers in information sharing is small.

4.2.5 Evolved Threat landscape

Primary focus of SOCs and MSSPs will be on highly automated threats coming from skilled threat actors such as criminal organisations and State Actors.

For business End-users, threat actors on 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 threat actors are detected and mitigated automatically or handled as part of normal IT operations. Considering the profits that can be made, most attacks on End-users come from criminal organisations. But geo-political instability also triggers many state-sponsored attacks, with the aim to de-stabilize society or steal information. So the primary focus of SOCs and MSSPs is on these complex and serious attacks. Such attacks are always AI-assisted, and mostly targeting a specific End-user, which makes them hard to detect and mitigate.

4.2.6 High influence of Government Regulations resulting in formally accredited SOC services

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. On national level this has led to national cyber security regulations. These regulations 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 are available in the world. As a result, most End-users make use of certified SOC services.

4.2.7 Repositioned NCSC in the context of SOC functionality

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.

NCSC will act 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 the large technology providers that feed the NCSC with threat information. Relevant information is distributed by the NCSC to sectoral SOCs, End-user SOCs, MSSPs and MSPs. The other way around, sectoral SOCs, End-user SOCs, MSSPs and MSPs share relevant information with the NCSC. When an incident with societal impact occurs at an End-user in a critical sector or at several End-users simultaneously, the NCSC will coordinate the mitigating actions over all End-users on a national level.

4.3 SOC and SOC environment

In this paragraph, the different aspects of the blueprint of the SOC of the future itself will be described.

4.3.1 SOC mainly in proactive role

The SOC focus is largely on proactive and predictive activities

Most known security incidents and vulnerabilities get detected automatically and mitigation is largely standardized and automated, for instance implemented with support of security playbooks and SOAR tools. These playbooks and tooling of course need to be maintained, this is typically an security engineering task. In (Daniel Schlette, 2024) an empirical assessment 1217 playbooks, an online study with 147 participants, and in-depth interviews with nine security professionals led to the conclusion that there are intrinsic ambiguities in the way practitioners and organizations define their playbooks. Also available playbooks cannot be used outright which might currently impair their wide use across different cybersecurity actors. Despite the availability of playbooks, 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. The goals are to be optimally prepared for upcoming attacks and be able to implement measures that will either prevent such attacks or reduce the impact of such attacks. This way of working will have an impact on the SOC staffing (see par. 4.3.6).

4.3.2 Highly automated SOC technology & tools

All Information security incident and vulnerability discovery activities and most mitigation and recovery, vulnerability response and data acquisition 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. This high level of automation has replaced first- and second tier security analysts in all but a very few (specialized) SOCs and for new and/or sophisticated attacks. The shift to cloud services (see par 4.2.4 below) offers potential for automated response. SOC personnel are able to focus on predictive and pro-active activities, business risk and situational awareness through a highly integrated single pane of glass. The foundation of these activities constitutes an interconnected security data lake, filled by many different internal and external data and information sources, maintained by data engineers.

4.3.3 SOC supports Business processes

Business processes, such as Zero Trust decision making, benefit from the wealth of information that is available at the SOC.

A SOC gathers an enormous amount of up-to-date information and data from all infrastructure and applications of an End-user. This information is needed for the automated detection and response, creating situational awareness and proactive and predictive way of working. Other business processes also profit from this information. For instance the 'continuous decision making' in Zero Trust will highly benefit from the up-to-date information sources available at the SOC. For example the information can be a trigger to decide to instantaneously change access rights that have been previously granted to an employee or application.

4.3.4 High degree of standardized solutions

Highly standardized technology, tooling and a way-of-working enables efficient and effective performance and information exchange.

SOCs and MSSPs make elaborate use of the widely available standards, such as for incident data formats, information exchange formats, maturity models, and cloud APIs descriptions. Because of the use of these standardized formats and interfaces, the way of working is efficient and tools are interchangeable.

4.3.5 Infra under monitoring mostly cloud based

Most of the infrastructure that is monitored by SOCs and MSSPs will be cloud-based.

The whole IT-services industry has successfully transitioned to a “cloud unless” approach, leaving only classified systems (e.g. processing state secret information), highly vulnerable intellectual property and OT as remaining on-prem assets. Also ‘Cloud Edge’ solutions are broadly used, in which cloud technology is used on location, for example in combination with OT. This means that cloud security strategies are the main focus of SOC personnel. Having such a large portion of assets in the same (cloud) environment 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.

4.3.6 Staffing

A majority of SOC staff will consist of Risk analysts, Data analysts, Threat analysts and crisis managers; only very few ‘traditional’ SOC analysts are needed.

Virtually all traditional Tier 1 and Tier 2 SOC analysts have been phased out, 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 core SOC services, such as collecting and processing high quality TI-data, establishing Situational Awareness and predictive analysis, risk assessment and determination of Course of Action. Since the focus has shifted to responding to threats instead of incidents, response staff consists mostly of security engineers (e.g. developing and operating automated response technologies) rather than traditional incident responders. For crisis scenario’s, where imminent cyber threats seriously endanger business continuity, crisis managers are assigned to align with decision makers from the business. A challenge is to find and/or educate the few SOC analysts that are still needed, considering the traditional career path from Tier 1 to Tier 2 to SOC analyst expert has disappeared.

4.3.7 Internal organisation and mandate

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. With the shift to a predictive and proactive approach, SOCs have received the mandate for making pre-emptive changes to the IT environment. A business impact threshold is agreed upon above which additional authorization needs to be sought from decision makers. This goes for organisations with an inhouse SOC as well as MSSPs.

5 Recommendations

Based on this research, the following recommendations are defined for the relevant SOC-stakeholders: Government, NCSC, Organisations with inhouse SOC capabilities, MSSPs, and MSSP customers.

One general recommendation to all stakeholders is to focus more on collaboration and sharing of information. In the interest of National Security and the resilience of society, collaboration and the exchange of information is key. It is essential for SOCs to focus more on pro-active and predictive capabilities, which can only be successful when done in collaboration. Therefore, building new collaborations and expanding existing collaborations is recommended; assessing together how knowledge, experience and data can be shared and used for mutual benefit.

Government

Most interviewed experts believe more guidance and more enforcement are required from government institutions. Many organisations, especially smaller companies, need this to initiate the necessary actions and activities on cyber security in general, including their SOC activities. Government agencies should prepare for such stronger enforcement role, which of course is supported by upcoming EU regulations such as NIS2. Enforcement policies should reflect both the advancements in cyber security threats and the pace in which the market can operate. In general, government institutions are urged to ramp up their cybersecurity efforts, to set clear targets for government and collaborative initiatives and communicate more clearly on their intentions. Joining forces with the experts, and making this a public-private collaborative effort, is recommended.

NCSC

There is a lot of uncertainty among the interviewed experts on what can be expected from the NCSC, both now and in the future. The NCSC is mentioned as an institution ideally suited to play a central role in information exchange and sharing, enabling (sectoral) collaboration and other important tasks in the coming years. The recent merger between the Digital Trust Centre (DTC) and NCSC is a good step in expanding the scope of the NCSC. Also the coordinating role of the NCSC in national cyber crises is considered to be important. Some experts even suggest that the NCSC should take on an operational role (implementation) for sectors that lack the expertise and/or resources and capabilities to implement SOC capabilities themselves. However, more credible is that the security market assumes such an operational role, and not the NCSC. Further definition of the NCSC mandate within central government is recommended, given the developments on (EU) regulation, threat landscape and geopolitical situation. It is also recommended to decide on whether the NCSC should act as National SOC, as defined in the Cyber shield regulations[8]. Finally, it is very important to communicate clearly on what the stakeholders can expect from the NCSC.

Organisations with in-house SOC capabilities

The following questions should be regarded for determining an inhouse SOC strategy for the coming years:

[8] https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

- Can the required level of funding, and the number and competency of personnel for your SOC be consistently secured, to keep up with developments in technology, threat landscape, and regulations?
- What will the impact be of further migration to cloud infrastructures on your SOC capabilities?
- Can keeping your own independent SOC be justified? Could replacing (part of) your SOC capabilities by MSSP-market alternatives or even MSP or vendor built-in security capabilities provide a better, more cost-effective solution? What will the impact be on the transparency of your operations and on your (security) sovereignty?

MSSPs
The following questions should be regarded for determining the MSSP SOC services strategy for the coming years:

- Will you be able to consistently offer high-quality and cost-effective SOC services to your customers, given the developments within MSPs and Technology providers, regarding technology, the threat landscape and regulations?
- What impact will further migration to cloud infrastructures have on the SOC services you offer?
- How will your collaboration with Technology providers and MSPs be shaped?
- How can you ensure that your SOC staffing and internal organisation undergoes a smooth transition?

MSSP customers
It is recommended to continually consider the added value of the services provided by the MSSP, and how this holds up to the capabilities of MSPs or (cloud) technology providers. Organisations that desire to be completely unburdened could outsource their infrastructural and security services to an MSP or a combination of an MSP and an MSSP; this does however come with a reduced transparency and sovereignty. When (partially) outsourcing SOC capabilities, focus on service levels that incorporate risk and impact, instead of on the number of resolved incidents. Actively govern your service provider using established metrics to monitor and improve the service provider performance and alignment with your organisation. Prepare for a shift from a responsive SOC to a proactive SOC, as this will require your organisation to provide your service provider (whether MSSP, MSP or other type of provider) with a broader mandate.

References

(ISC)2. (2022). *Cyber security workforce study.*

Baines, V. a. (2021). *Project 2030 - Scenarios for the Future of Cybersecurity.* Opgehaald van https://resources.trendmicro.com/rs/945-CXD-062/images/WP01_Project%202030_White%20Paper_210505US_Web.pdf?_ga=2.257945291.1928719772.1702548469-1811587288.1696418073

Bussier, F. (2023, September 20). Guide: Large Language Models-Generated Fraud, Malware, and Vulnerabilities. Opgehaald van https://fingerprint.com/blog/large-language-models-llm-fraud-malware-guide/

Daniel Schlette, P. E. (2024). Do You Play It by the Books? A Study on Incident Response Playbooks and Influencing Factors. *2024 IEEE Symposium on Security and Privacy (SP)* (pp. 60-60). IEEE computer society.

Deloitte, GoogleCloud. (2020). *Future of the SOC - Forces shaping modern security operations.*

Edgars Taurins. (2020). *HOW TO SETUP UP CSIRT AND SOC.* European Union Agency for Cybersecurity (ENISA). doi:10.2824/056764

ENISA. (2023, March). *Identifying emerging cyber security threats and challenges for 2030.* Opgehaald van https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030/@@download/fullReport

Erzberger, A. (2023, August 8). WormGPT and FraudGPT – The Rise of Malicious LLMs. Opgehaald van https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/wormgpt-and-fraudgpt-the-rise-of-malicious-llms/

European Commission. (2020). *Call for Expression of Interest (CEI) to select entitie that provide the necessary facilities to host and operate Cross Border Platforms.* https://cybersecurity-centre.europa.eu/system/files/2022-11/Call%20for%20Expression%20of%20Interest_Cross-border%20SOC%20platformsfinal.pdf.

FIRST. (2019). *Computer Security Incident Response Team (CSIRT) Services Framework, version 2.1.* Forum of Incident Response and Security Teams, Inc. (FIRST.Org). Opgehaald van https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Iman Ghanizada, D. A. (2021). *Autonomic Security Operations.* Cyber Security Action TEam, Google Cloud.

Jansen-Ferdinandus. (2018). *IMPROVING HUMAN CAPITAL: A COLLECTIVE NEED FOR INDIVIDUAL COMPETENCIES.*

Johnson, K., & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intelligent Automation and Soft Computing (IASC) Vol.28, issue2, 28*(2). doi:10.32604/iasc.2021.016240

Kathryn Knerler, I. P. (2022). *11 strategies of a world-class Cybersecurity Operations Center.* MITRE Cooperation.

N. Brownlee, a. E. (1998, June). RFC 2350 - Expectations for Computer Security Incident Response. IETF. Opgehaald van https://datatracker.ietf.org/doc/html/rfc2350

NCSC. (2023). *Facsheet SOC inrichten: begin klein - Start vanuit eenvoud, groei vanuit behoefte.* The Hague: NCSC.

Oldengarm, P. (2023). *Een beleidskader voor het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland.* Stuurgroep voor de versterkte aanpak vitaal (VAV).

Paganini, P. (2023, June 14). LLM MEETS MALWARE: STARTING THE ERA OF AUTONOMOUS THREAT. Opgehaald van https://securityaffairs.com/147447/malware/llm-meets-malware.html

Sadasivam, S. C. (2018). Efficient reinforcement learning for automating human decision-making in soc design. *Proceedings of the 55th Annual Design Automation Conference* (pp. 1-6). IEEE.

SOCCRATES, p. (2022, September). *SOCCRATES Vision paper.* Opgehaald van www.soccrates.eu: https://www.soccrates.eu/wp-content/uploads/2022/05/soccrates_vision_paper_downloadable.pdf

TNO. (2023). *Checkmate, cyber security?* TNO.

Van Os, R. (2023, March 22). No more Tiers. Opgehaald van LinkedIn.com: https://www.linkedin.com/pulse/more-tiers-rob-van-os/

Van Os, R. (2023, October 18). The AI driven SOC: a glimpse into the future of security operations. Opgehaald van https://www.linkedin.com/pulse/ai-driven-soc-glimpse-future-security-operations-rob-van-os/

Zimmerman, C. (2022). *Eleven Strategies of a World-Class Cybersecurity Operations Center.* The MITRE Corporation.

Appendix A - List of interviewees

Table 1: list of interviewees

Name	Role	Organisation
Richard Strooper	CTO	Pinewood
Remco Sprooten	Senior Research Engineer	Elastic
Philip Hebly Jelle Niemantsverdriet	Partner development National security officer	Microsoft
Etienne Kuijkhoven André Oosterwijk Michel Zoetebier	Manager Blue team ((SOC, CERT & abuse) Senior SOC analist Senior SOC analist	KPN
Petra Oldengarm	Director Independent Cyber Security Advisor Author of 'CSIRT-STELSEL'	Cyberveilig Nederland
Richard Kerkdijk Frank Fransen	Senior Cyber Security experts	TNO
Rob van Os	Owner of SOC-CMM	SOC-CMM
Jelle van Hengel	Manager Operations	Fox-IT
Jenny Gershkowich	Head of the Security monitoring and incident response	ABN AMRO

Appendix B – Glossary and terminology

Glossary

AI – Artificial Intelligence
API – Application Programming Interface
CEI – Call for Expression of Interest
CERT – Computer Emergency Response Team
CSIRT – Computer Security Incident Response Team
DTC - Digital Trust Centre
ISAC – Information Sharing and Analysis Centre
IT – Information Technology
IoT – Internet of Things
LLM – Large Language Model
MSP – Managed Service Provider
MSSP – Managed Security Service Provider
OT – Operational Technology
SOAR – Security Orchestrationm, Automation and Response
SOC – Security Operations Center

Terminology

Cyber Shield: The EU Cyber Solidarity Act aims to strengthen capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks. The proposal includes a European Cybersecurity Shield, made of Security Operation Centres interconnected across the EU, and a comprehensive Cybersecurity Emergency Mechanism to improve the EU's cyber posture (https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity).

Deception technology: a category of cyber security defense mechanisms that provide early warning of potential cyber security attacks and alert organizations of unauthorized activity. Deception technology enables a more proactive security posture by seeking to deceive an attacker, detect them and then defeat them.

Digital twin: "a digital model of an intended or actual real-world physical product, system, or process (a physical twin) that serves as the effectively indistinguishable digital counterpart of it for practical purposes, such as simulation, integration, testing, monitoring, and maintenance." (Wikipedia)

End-user: company or (government) organisation that has its own SOC or that makes use of the services offered by MSPs and MSSPs but also uses tools and products that are offered by Technology providers and Security vendors. Examples are ABN AMRO, KPN, ING, ASML. (Project team)

IoT: The Internet of things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks[9]

Managed Security Service Provider (MSSP): Service Provider that offers security services to their customers. These services often make use of the security technology of **security vendors** and apply it to the security of the IT infrastructure that is offered by **MSPs** and **Technology providers**. Examples are KPN Security, Fox-IT, Pinewood. (Project team)

Managed Service Provider (MSP): Service provider that offers IT services to its customers. These services often make use of the technology that is offered by **Technology providers.** Examples are Perium, Akamai, Forescout. (Project team)

OT: Operational Technology is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events[10]

Quantum computing: "Quantum computing is a rapidly-emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers." (IBM)

Security vendor: a company that offers dedicated security products and solutions. Examples are Fortinet, SentinelOne, Imperva (Project team)

Technology provider: a large tech firm that develops and offers IT infrastructure technology as a service. Examples are Microsoft, Google, Amazon. (Project team)

Zero-day: "A previously unknown hardware, firmware, or software vulnerability." (NIST)

Zero Trust: "A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised." (NIST)

[9] https://en.wikipedia.org/wiki/Internet_of_things

[10] https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

Distribution list

TNO Publiek | ONGERUBRICEERD Releasable to the public) TNO 2023 R11803

ICT, Strategy & Policy

Zernikelaan 17
9747 AA Groningen
www.tno.nl