SOC CMM

FIRST ANNUAL

SOC maturity report

Trends and insights in global SOC maturity

MAY 2025

SOC-CMM®

Table of contents

Foreword

This report represents the first annual SOC-CMM publication on SOC maturity. The mission of SOC-CMM is to improve security operations globally, and this report presents insights and trends in the SOC landscape that we believe are important for security operations teams.

The SOC-CMM model and assessment tool was introduced in 2016, after completing research on SOC maturity and capability, as part of a master's degree in information security. Its global adoption has meant that SOC teams around the world are leveraging the insights from their assessments to continuously improve their maturity and capability, and thereby resilience to cyberattacks.

In 2023, professional services for SOC-CMM were launched, with the introduction of the support partner network and the SOC-CMM Certified Assessor training. This training has been completed by over 200 people.

In the past year, many advancements were made for SOC-CMM. The first joint publication with the support partners was launched: the SOC-CMM metrics suite. The Lead Auditor training was introduced, the SOC certification program was launched on October 31st, and the support partner network was extended from 7 to 17 partners (and currently on 22) to ensure global availability of support for strategic SOC advisory services, including SOC-CMM assessments.

This year, with the introduction of this report, SOC-CMM is taking another step in professionalising services and products to the SOC community. This report aims to inform SOC teams of current maturity state, trends, expectations and needs of the SOC community, as well as upcoming changes to SOC-CMM products and services.

We hope you enjoy reading this report. As always, and in line with the principles of SOC-CMM, your feedback is much appreciated.

On behalf of SOC-CMM and the support partners,

Rob van Os
Strategic SOC advisor & Director
SOC-CMM

Management summary

This report presents findings from the first SOC-CMM maturity survey and combines these findings with maturity data collected in the support partner network, and observations from SOC-CMM and the support partners. For SOC-CMM, this report represents the next step in providing valuable resources to the SOC community.

This report contains information on maturity scoring across different regions, sectors, and SOC sizes and types. Important conclusions on maturity growth over time, differences in maturity between SOCs, and differences between outcomes of self-assessments and third-party assessments are presented. The information on this topic can be used by SOCs for high-level benchmarking purposes (more detailed benchmarking is available through support partners), and to align their strategies with common SOC challenges. The main conclusion from the maturity section is that enhancing maturity in the SOC requires focus and commitment. Challenges with the execution of maturity assessments, and overestimation of maturity in self-assessment, are likely contributors to lack of maturity growth.

This report also contains information on the outcomes of the SOC-CMM maturity survey. Part of the survey inquired about maturity scores (covered in the State of SOC maturity section). Additional questions were asked about implementation strategies and design decisions within security operations centers. The outcomes show commonalities between SOCs on certain topics and differences between SOCs on others. This information provides insight into where SOCs are aligned on strategy, and where strategies lack best practices and a unified approach.

Also, the current state of the SOC certification program is shown, backed by data from the survey. This shows that there is much interest in the program across different regions. Objective demonstrability of SOC maturity and capabilities is an important driver for SOC certification. This is true for MSSPs that want to demonstrate this to their clients and prospects, but also for in-house SOCs, that wish to demonstrate SOC maturity to the board of directors and their constituency.

Additionally, the report looks at the next steps for SOC-CMM. Further extension of the support partner network in multiple regions and countries is expected. Additionally, an updated version of the SOC-CMM model will be introduced this year, with enhancements aligned with the needs of the SOC community. This updated version of the model will be accompanied by an updated version of the SOC-CMM assessment tool. Additional improvements in the SOC-CMM product portfolio are also discussed in this section. An important improvement is the intended creation of a library of best practices, where topics that are challenging to SOCs will be discussed between SOC-CMM and the support partners to present common challenges and possible solutions.

Lastly, support partner insights are also shared, with each support partner presenting their observations of the SOC market, with identified trends and changes in customer demands. As different partners operate in different regions and countries, their insights vary as well.

In short, this report contains insights into security operations centers across a variety of topics that SOCs can use to compare themselves against. SOC can also use the information in this report to learn from and adopt it into their strategies wherever applicable.

CHAPTER 1

Background

The next chapters will provide information on the state of SOC maturity and the outcomes of the SOC-CMM survey. To correctly interpret those findings, the chapter first explains the background of the SOC-CMM model, and the data used to create this report.

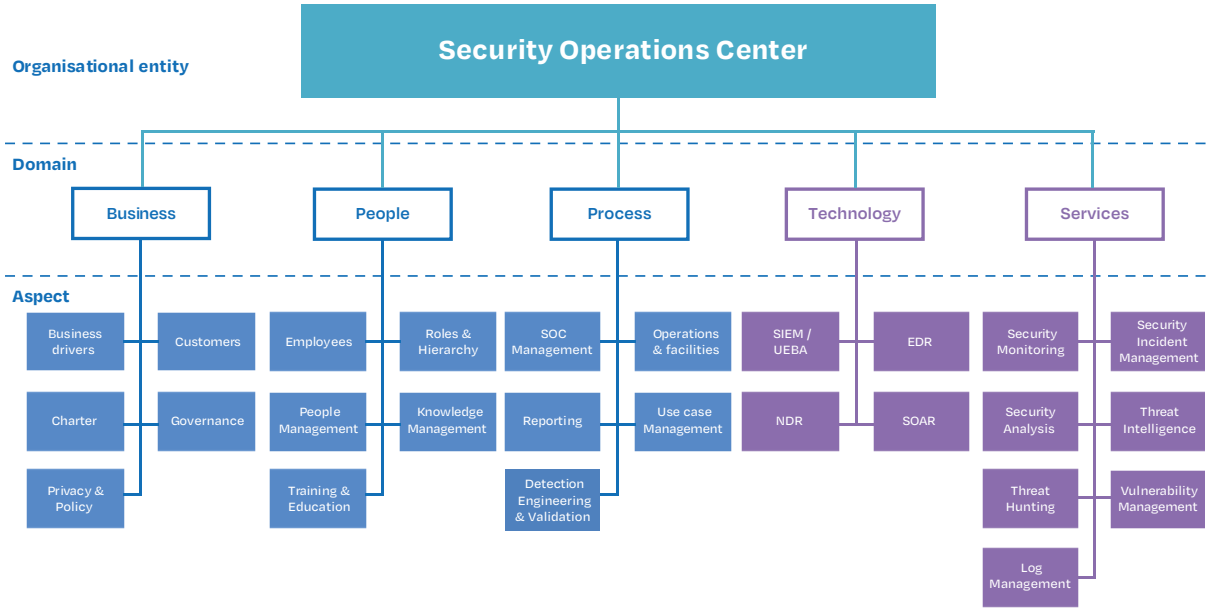
Background

SOC-CMM model

For discussing the state of SOC maturity in this report, the SOC-CMM model is used. This model, which is the basis for both maturity and capability assessment, as well as the certification program, has the following features:

- **5 domains.** The model has 5 domains for assessment. These domains are business, people, process, technology and services.
- **26 aspects.** The model has 26 aspects in total within the 5 domains mentioned. Each of the aspects represents a part of SOC operations.
- **6 maturity levels.** SOC-CMM uses 6 levels to establish maturity across all aforementioned domains, from 0 to 5. Maturity levels in SOC-CMM are continuous, rather than staged. This means that intermediate maturity levels are also allowed, resulting in more granular and organic growth.
- **4 capability levels.** SOC-CMM uses capability levels to establish capability across the technology and services domains. Like maturity, capability levels in SOC-CMM are continuous, resulting in detailed scoring and growth potential.

The model is shown in the figure below. Blue represents the domains where only maturity is assessed, purple represents the domains where both maturity and capability are assessed.



Report data

The observations and figures presented in this report are based on maturity data and survey data. While there is an overlap, this is not the same data source, as explained hereafter.

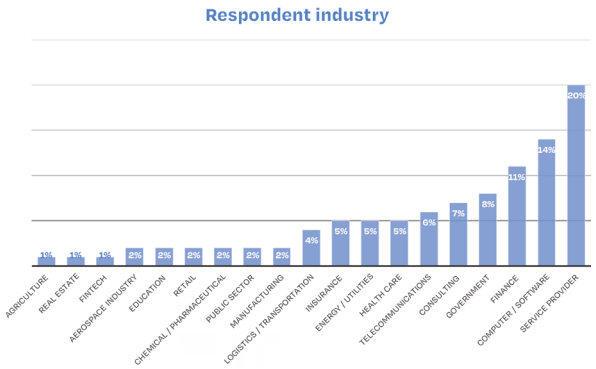
Maturity data

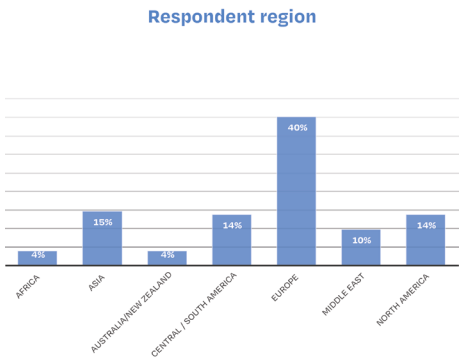
The graphs and observations about maturity scores presented in this section of the report are based on data from several sources:

- **Support partner data.** Support partner data accounts for 45% of the total data. Because support partners are trained and experienced in performing assessments and interpretation of questions, this data is the most trustworthy data to use.
- **Survey data.** Survey data accounts for 51% of the total data. Part of this data is based on self-assessment or 3rd-party assessment, part of the data is based on estimations of maturity, rather than actual assessment. The survey data is a little less granular, as the survey only allowed integers as maturity levels (scoring in SOC-CMM assessment is up to 2 digits).
- **Public submissions.** Public submissions represent 4% of the total data. The SOC-CMM assessment tooling contains a section on sharing results. This allows an organisation to share aggregated information from the survey, that is entered into the anonymised benchmark. Public submissions have so far been limited but are very valuable for reporting and benchmarking purposes.

Survey data

The survey data was collected in the period of end of January to mid-March 2025. The survey was filled in by approximately 200 people. To put the outcomes of the survey in the correct perspective, it is important to understand the population of the respondents. This is represented in terms of industry and region.





Bias

To put the data into the right perspective, it is important to understand any bias in the data set. Two questions were asked in the survey to uncover any bias. The first question was about where the person answering the survey found the survey. In total, 38% learned about the survey through SOC-CMM directly, either through the website, or through the mailing list. The other 60% learned about the survey through other means, such as LinkedIn, or via others. This means that the majority was not directly targeted.

The question inquired about previous usage of SOC-CMM. The fact that 60% of respondents have not actually used SOC-CMM before to assess their SOC, is an additional indication that the data set is not biased to those who already have an established practice of SOC maturity measurement. Of course, those who have not performed (self-)assessment before, are limited to estimating their maturity scores, rather than basing them on actual assessment data.

Report structure

This remainder of this report consists of 5 chapters. In the first chapter, the state of SOC maturity is discussed. In the second chapter, SOC challenges and design choices are discussed to highlight similarities and differences in SOC implementation. The third chapter addresses SOC certification, and the current status of the certification program. Chapter four discusses the roadmap for SOC-CMM in the next year. Finally, chapter five outlines the insights and observations from the SOC-CMM support partners.

CHAPTER 2

State of SOC maturity

This chapter of the report focuses on the observations based on the maturity data collected from the survey and the support partner network and focuses on difference in maturity, maturity growth and development, and mature-related questions from the survey.

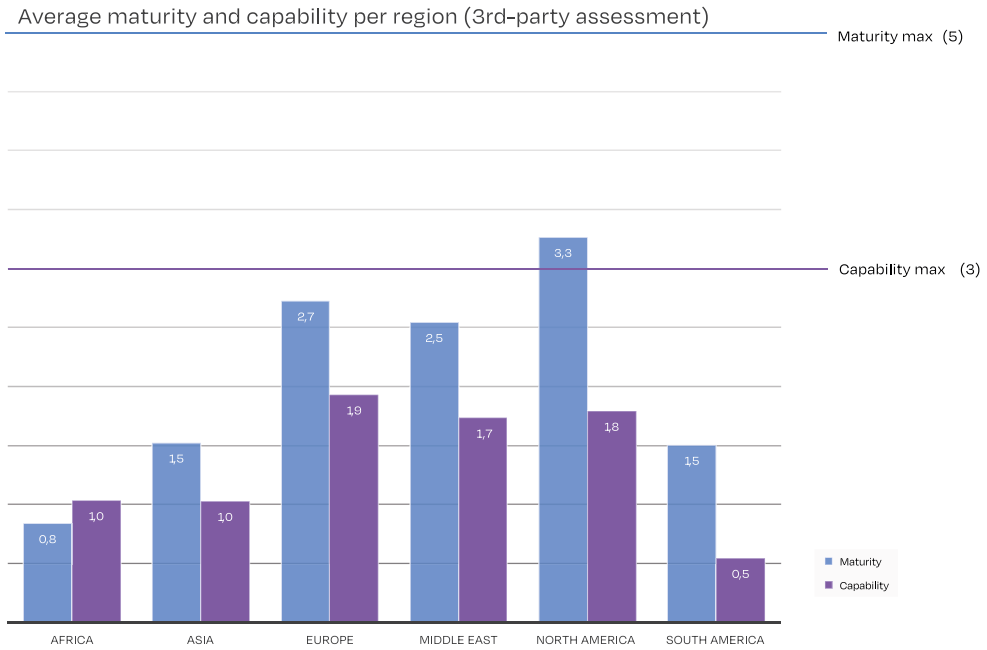
State of SOC maturity

Maturity differences

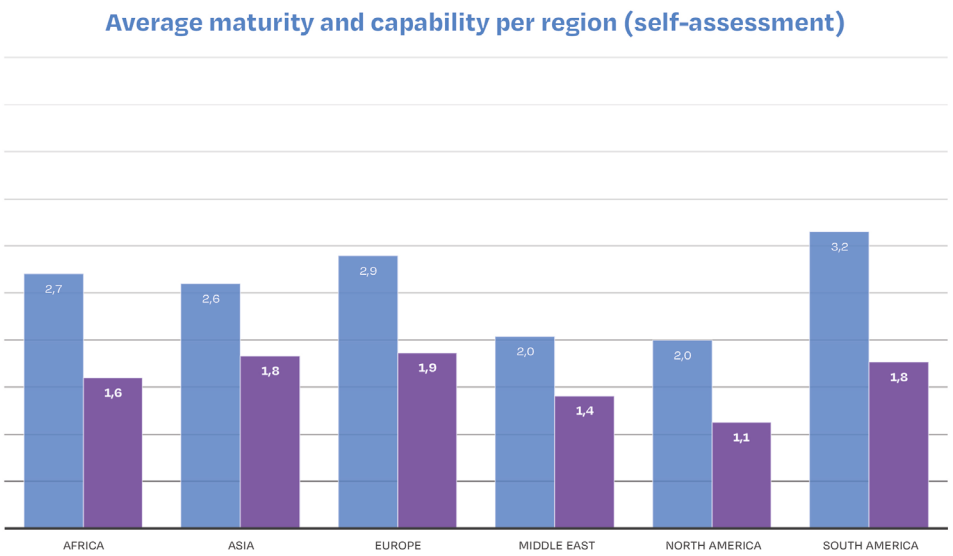
Using the data, differences between regions, sectors, and SOC types were observed. It must be noted that for Asia, Africa, and South America, the number of data points is more limited than for the other regions. SOC-CMM will invest in gathering additional data points, that will provide a more accurate picture of these regions.

Maturity and capability per region

The following figure shows the average maturity and capability per region according to the data collected by the support partners. Blue represents maturity scoring, green represents capability scoring, as indicated in the legend. The figure also contains the maximum scores for maturity (5) and capability (3). This is only done for the first graph; the reader should take these different scales into account when reading the next graphs as well.



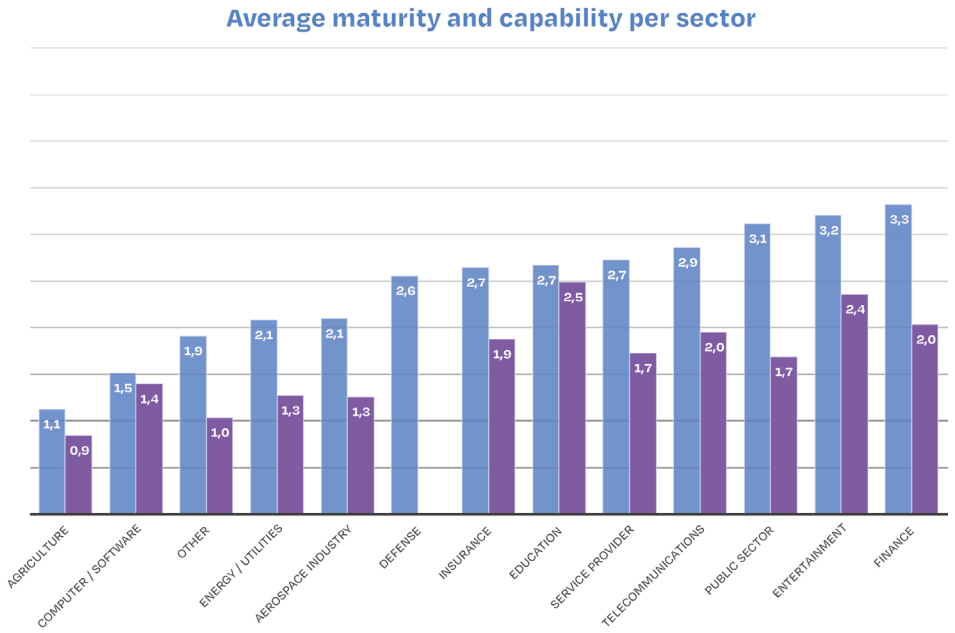
When comparing this data with the self-assessment and estimation data, big differences were seen with the support partner data. The resulting number are almost an inverse of this graph, with Africa, Asia and South America having the much higher scores (as demonstrated below).



This deviation may result from unfamiliarity with the model and the practice of self-assessment, resulting in over-estimation of maturity in some regions. Interstingly enough, self-assessments from the Middle East and North America result in lower scoring, possibly indicating a too critical approach to self-assessment.

Maturity and capability per sector

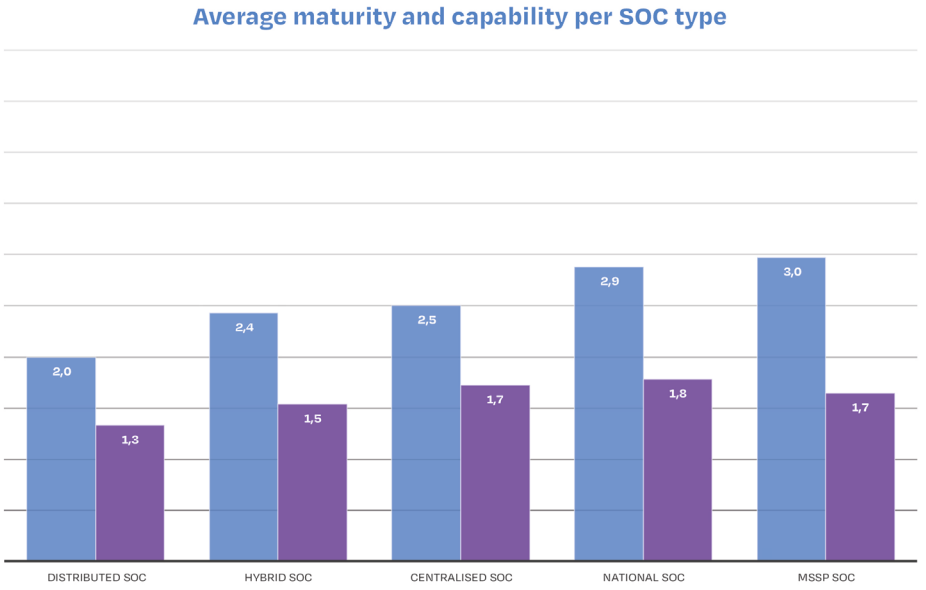
Differences are also observed between sectors. From this graph, it is also visible that higher maturity levels are associated with higher capability levels. Education, in this case, is an obvious outlier, as its capability level is almost equal to its maturity level. Note that 'Defense' has no capability scoring. This is because data points for this sector are currently limited, and no capability scoring is available.



As expected, more regulated sectors generally score higher for both maturity and capability. While there are differences observed between the support partner data and the other data, the top scoring sectors are almost the same.

Maturity and capability per SOC type

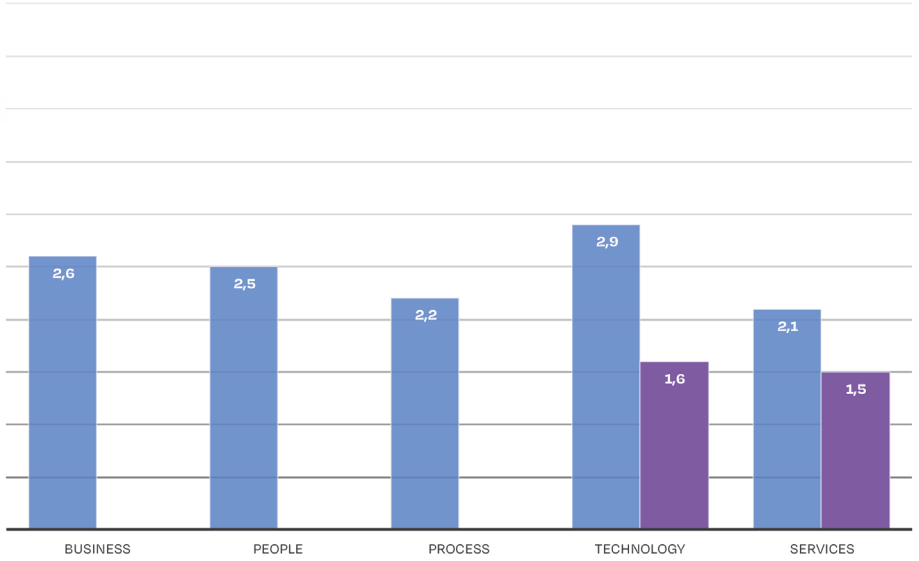
In the 11 Strategies of a World-class Cybersecurity Operations Center publication by MITRE, different SOC types are introduced. These SOC types are also used in the survey and the SOC-CMM tooling to create a SOC profile. The following figure shows the average maturity and capability per SOC type. Note that centralised, distributed and MSSP SOCs represent the largest portion of the data. Accuracy for other types of SOCs, as a representation for the whole population, is likely lower.



Maturity per domain

Finally, difference in maturity can also be observed in the model itself (the domains). This will be shown in more detail in a later section of this chapter.

Average capability & maturity per domain



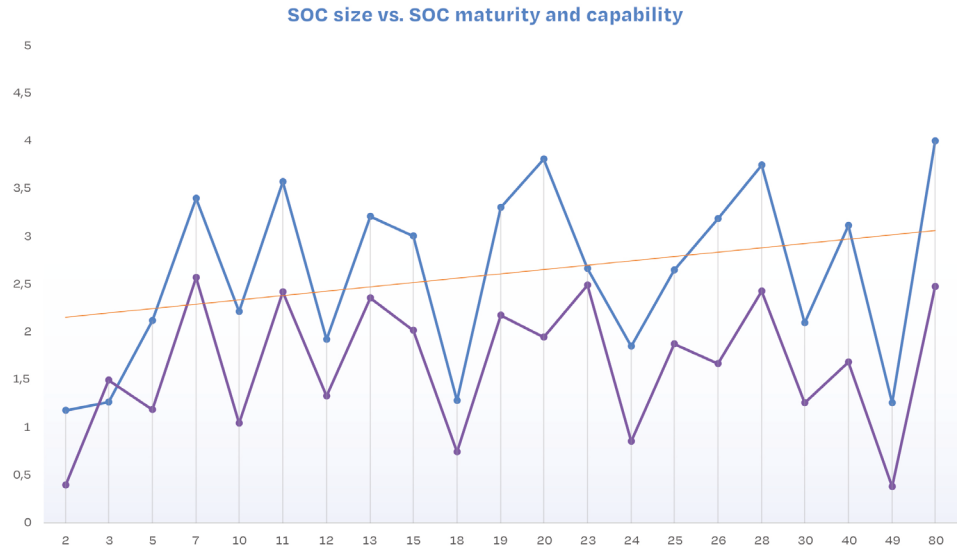
While differences between domains are not big, the technology domain is, on average, the most mature domain for many SOCs. This is likely because SOCs often start with technology, before moving into other domains. More detailed scores reveal that maturity in the service domain is negatively impacted the most by lower maturity of the threat hunting and threat intelligence services.

Maturity progression

Maturity progression can have a relationship to SOC size and the number of years that the SOC has been in operation.

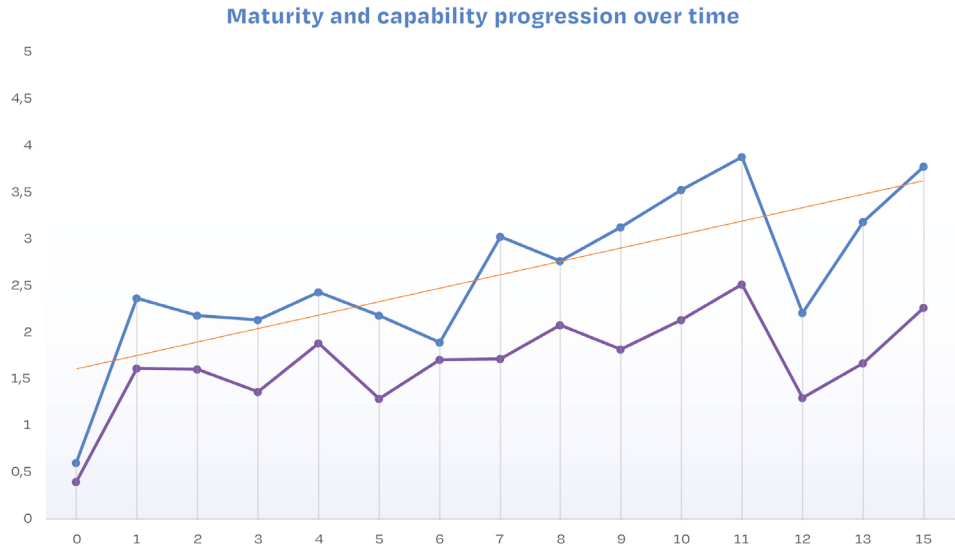
SOC size versus SOC maturity

When plotting the size of the SOC (in FTE) and the maturity of these SOCs, a very erratic pattern is shown. Small teams struggle with maturity and capability, but from 7 FTE onwards, there is no strong relationship between size and maturity. The maturity trendline (shown in orange) supports this, as there is an upward trend, but not a significant one. The horizontal axis shows the number of FTEs in the SOC.



SOC maturity over time

SOCs generally develop their maturity over time. Investing in maturity within the SOC requires insight into strengths and weaknesses, and applying improvements, either through a maturity improvement program, or as part of continuous improvement efforts in the SOC. The following figure shows the progression of maturity over time. The horizontal axis shows the number of years that the SOC has been in operation. The orange line represents the maturity trend.

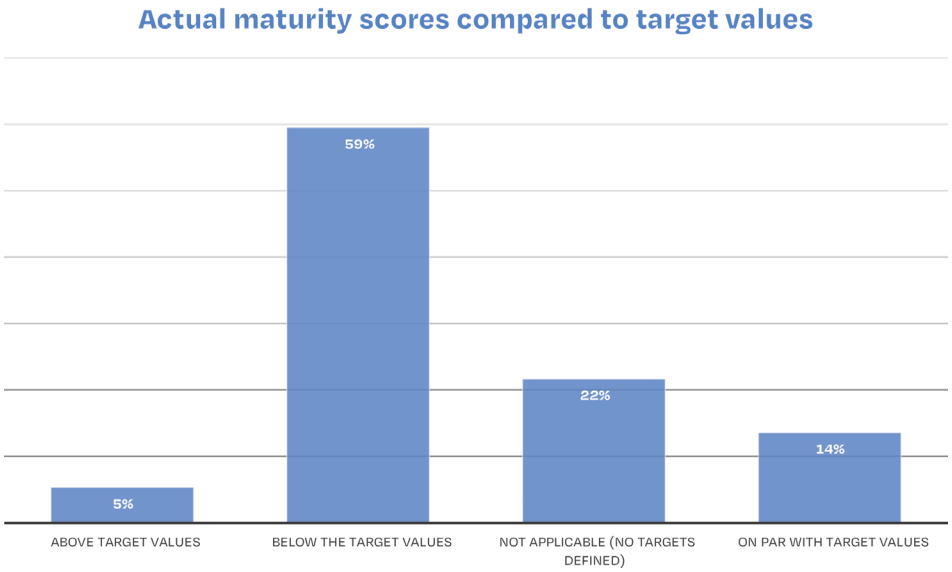


The development of maturity over time is comparable between self-assessment and third-party assessment. However, there are two identified differences:

1. Average maturity and capability are higher for self-assessments, as observed earlier
2. Third-party assessment results show a more gradual progression than self-assessment, which tends to be more erratic.

SOC maturity targets

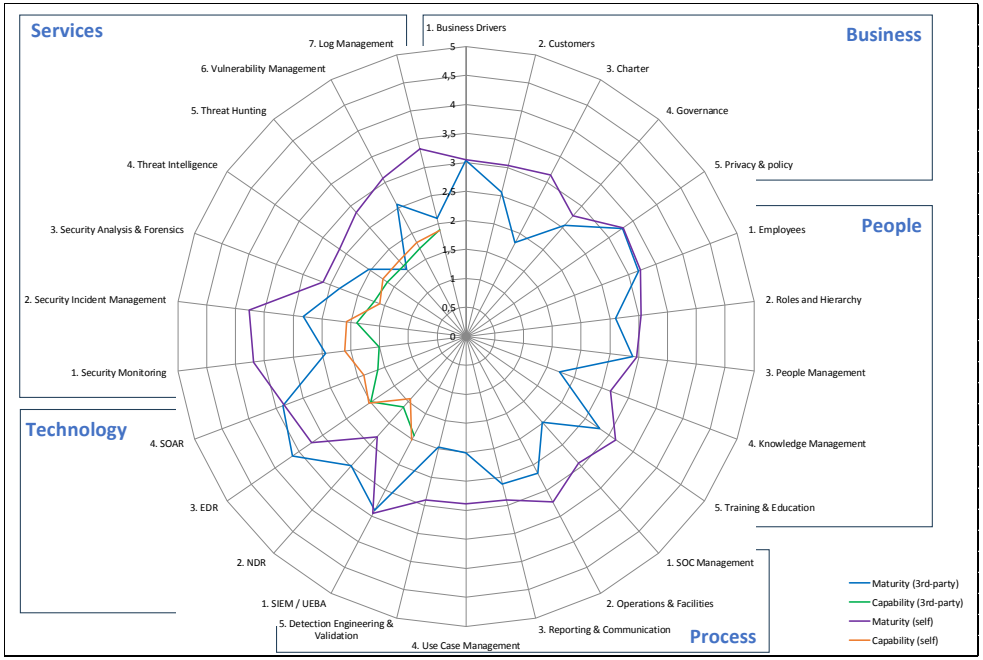
Part of the SOC-CMM assessment process is defining maturity targets to compare the current state against. Nearly 60% of respondents indicate that their current state is below the maturity targets. Only 19% of respondents indicate that current state scores either align with intended targets or even exceed those targets.



The last 22% of respondents have no target defined for maturity. While it is not a requirement to define targets, it makes sense to have a target in mind when scoring and growing maturity. For an initial baseline assessment, it may be difficult to set those targets as there is no reference point. In such a case, defining the target based on the intent of the maturity levels, or using the default SOC-CMM values (level 3 for maturity, level 2 for capability) are viable strategies.

Detailed SOC-CMM scores

The previous figures have highlighted differences between SOCs and the relationship between SOC size and age and maturity. The following figure presents a detailed view of SOC maturity for all aspects of the SOC-CMM domain, and the difference between 3rd-party assessment and self-assessment.



Overall, as stated before, self-assessment results in higher scores than 3rd-party assessment. This is true for both maturity and capability. Additionally, there are some more significant differences between these types of assessment. The biggest differences are in the following elements:

- Charter
- Knowledge management
- SOC management
- Use case management
- Detection engineering & validation
- The security monitoring, security incident response, threat hunting and log management services

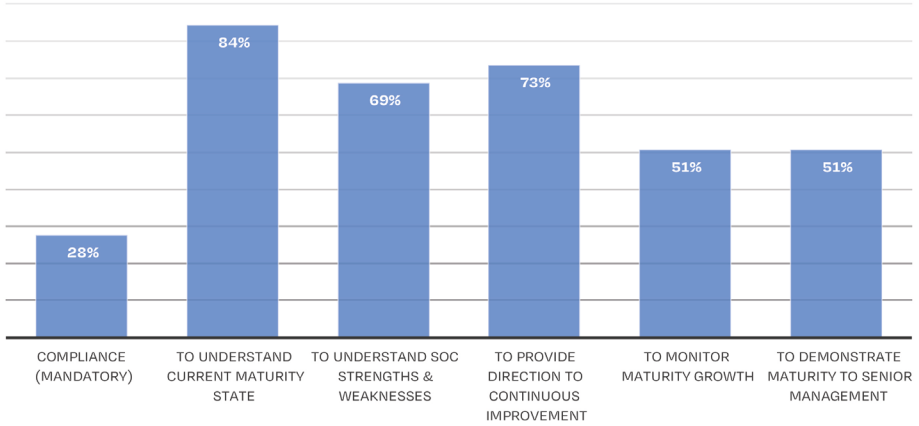
In practice, it is observed that many SOCs struggle to comprehend what maturity in many of these topics truly represents, and what artifacts are required to support this maturity. Failure to understand maturity for certain topics, can easily lead to overestimation of maturity. The SOC-CMM assessment tool provides input for these topics through the maturity questions, the supporting yes/no questions, remarks, and guidance.

Maturity assessment challenges

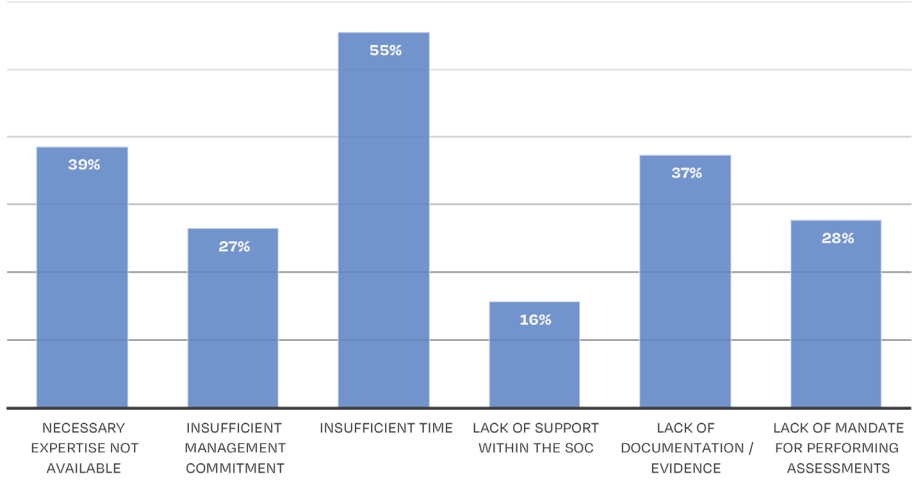
There are several reasons for SOC to perform maturity assessment. The main reasons are understanding current state, understanding strengths and weaknesses, and providing direction to continuous improvement. Compliance is the least common reason for SOC assessment, although this may increase as more SOCs are intending to get SOC-CMM certified (see chapter on certification).

SOCs face challenges when conducting SOC maturity assessment. The most common challenge in assessment is lack of time. While SOC-CMM support partners can reduce the time required to perform assessment and define follow-up roadmaps, it must be noted that even third-party assessment does require some commitment and resources from the SOC.

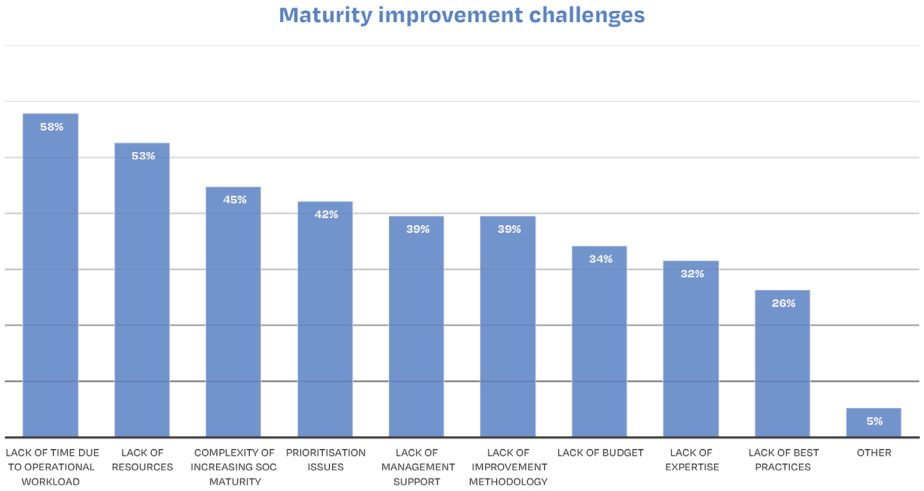
Maturity assessment reasons



Maturity assessment challenges



SOCs also indicate a number of challenges when trying to increase maturity in the SOC. The most common challenge is lack of time due to workload. While this is understandable, it also means that addressing the core issues that cause the workload becomes difficult. Dedicating a part of the time to improvement (capacity to improve) is an essential part of a successful continuous improvement strategy, even if it means making challenging decisions on SOC operations. Other common challenges include lack of resources, complexity and prioritisation issues. Essentially, these all come down to management decisions, that depend on vision and strategy in the SOC.



CHAPTER CONCLUSIONS

From the data presented in this chapter, the following conclusions can be drawn:

- For most SOCs, maturity gradually increases over time. However, it is not a given. Maturing a SOC does not happen by itself but requires insight and management support.
- Differences in maturity are observed in SOC sector, SOC type and SOC region. MSSP SOCs, SOCs in the financial sector, and SOCs in North America represent the SOCs with the highest maturity and capability scores.
- Self-assessment and estimations often result in overestimation of maturity levels. More accurate insight into maturity levels requires a more objective view.
- SOCs struggle with performing assessments, as well as dealing with the outcomes of assessment. While 3rd party assessment can partially solve this problem, commitment to improvement effort is required for successful maturity growth in the SOC.
- Supporting processes, such as use case management, knowledge management and detection engineering represent the biggest challenges for SOC maturity. This may be due to lack of best practices around these topics.

CHAPTER 3

SOC challenges and design choices

Besides inquiring about SOC maturity, maturity challenges and assessment challenges, the survey also contains a section on SOC design choices and implementation. This section was based on common challenges in SOCs that were observed over the last years within the support partner network. The structure of this chapter is largely aligned with the SOC-CMM model and presents the findings from the survey across the people, process, technology and services domain.

SOC challenges and design choices

People domain

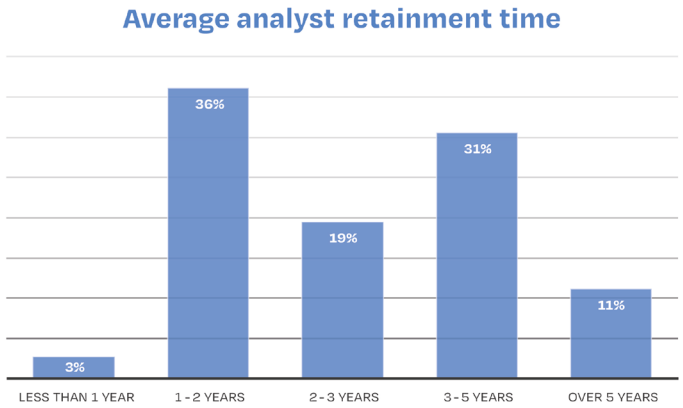
The people domain in the SOC-CMM model addresses maturity in relationship to staffing, roles, people management, knowledge management and training & education.

Employees

Challenges regarding employees are related to staffing within the SOC. Staffing levels themselves can be challenging; additional challenges come from maintaining staffing levels over time and attracting talent and senior staff.

Retainment and recruitment can be challenging for SOCs. SOCs are challenging environments to work in, with high workloads being common. Additionally, SOC work can be both stressful and repetitive.
Also, SOCs, and especially analyst positions, are often seen as a starting point for a career in cyber security. This is even more the case in organisations (such as MSSPs) that separate monitoring from incident response and follow-up, thereby limiting growth potential in the SOC.

These challenges may lead to lower retainment time. The survey shows that many SOCs have an average retainment of 1-2 years. This is relatively short, mostly because the investment in training and knowledge building is often significant for analysts. Fortunately, there are also many SOCs that have longer retainment periods.

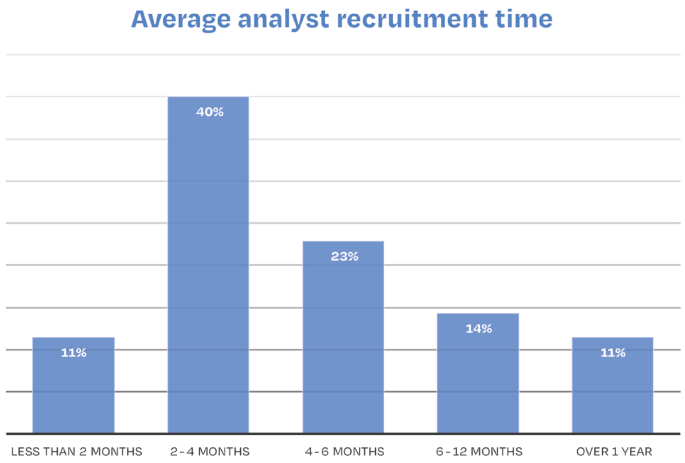


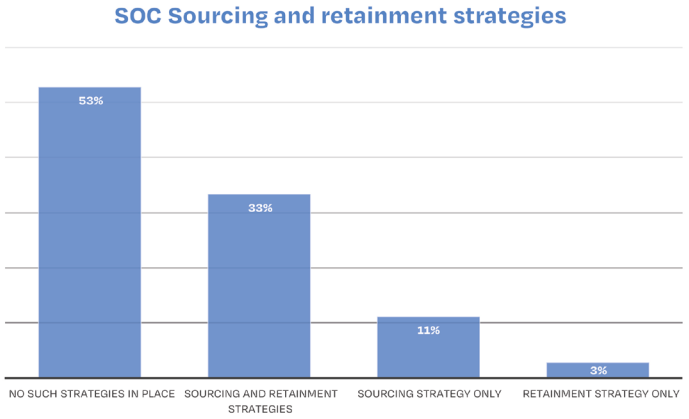
To counter loss of resources, an effective recruitment process should be in place. Most respondents indicate that the average recruitment time for analysts is around 2-4 months, which is a relatively short period of time. Anything over 6 months can be considered a long sourcing period. Especially if retainment times as relatively short (1-2 years), longer recruitment times can cause staffing level challenges. In such cases, optimisation of the recruitment process and implementation of a sourcing strategy can be beneficial.

A sourcing and retainment strategy represents a structured approach to attracting talent and ensuring that talent stays within the company. Such strategies are usually defined by HR, and should be tailored to the SOC.

The survey outcomes show that most SOCs do not have such strategies in place. For most organisations, this means that they rely on standard internal HR processes. Comparing sourcing and retainment time to the availability of strategy, we see that SOCs that have a strategy benefit from these strategies with shorter sourcing and longer retainment. However, the differences are not significant. This may mean that SOCs that have little trouble sourcing or retaining personnel (for example, due to market conditions, or other factors) have no need for such a strategy to be successful in this area.

Note: The survey did not differentiate between junior and senior analysts, so there is no data on this. However, from experiences seen in the support partner network, senior analysts are harder to source but generally stay with the organisation longer. Additionally, only analyst positions were inquired about. The reason is that every SOC has analysts, and not all SOCs have other roles defined (see next section).





Roles & hierarchy

Within the roles & hierarchy aspect, the survey inquired about the ratio between analysts and engineers and the application of tiering to the SOC.

Analysts versus engineers

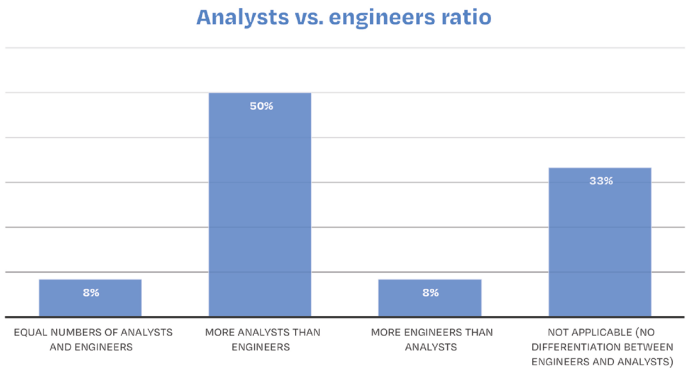
A security operations center can have many distinct roles for its employees. While many roles may exist, two roles have a particularly strong relationship: analysts and engineers (specifically: detection engineers and automation engineers). By investing in engineering, a SOC can reach higher levels of automation and more continuous detection improvement, resulting in more accurate alerts, therefore requiring less analyst capacity. Survey results indicate that more analyst than engineers or not differentiating between the roles is by far the most common ratio in SOCs.

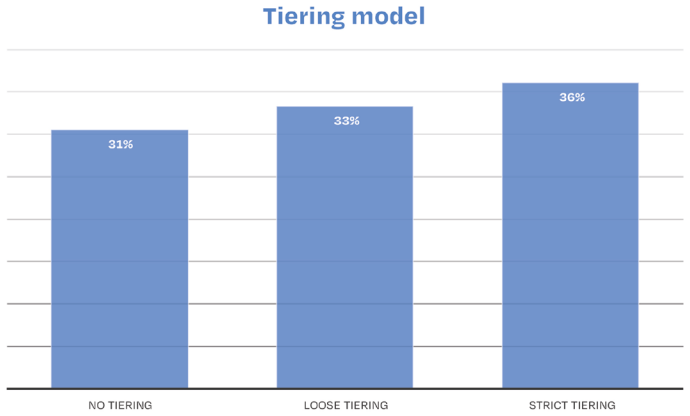
Having more engineers than analysts is not necessarily a sign of higher maturity. It usually designates a different approach to security operations; one that is more focused on SOC efficiency. The optimal ratio between analysts and engineers differs per organisation and should be aligned with strategy.

SOC tiering

Tiering in the SOC is still a point for discussion. While some SOCs use tiering to structure and standardise their operations, others believe tiering introduces unnecessary restrictions to analyst growth and development. The outcomes for the survey indicate an almost equal division between un-tiered, loosely tiered, and strict tiering. Loose tiering, in this case, means that there is tiering in place, but lower tier analysts can stay with in incident, and cooperate with higher tiers for full investigation, analysis, and resolving.

Similar to engineering versus analyst ration, tiering itself is not necessarily a sign of higher maturity; it depends on the implementation. Whether or not tiering is suitable to an organisation, depends on the requirements for the SOC, size of the SOC, SOC type and organisational culture.





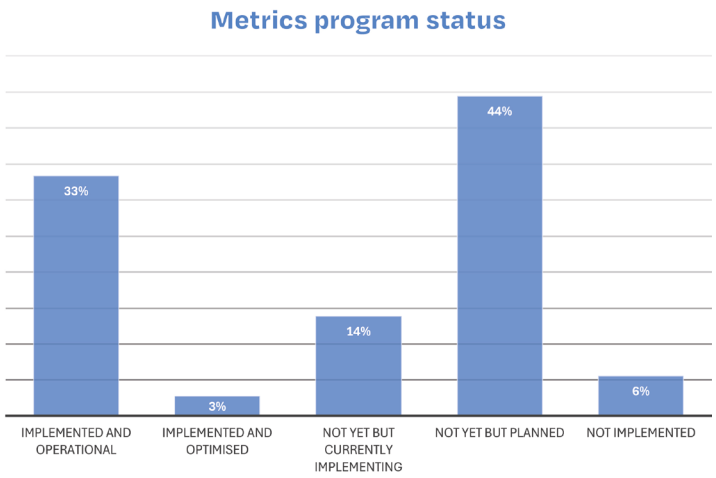
Process domain

The process domain in SOC-CMM deals with topics like SOC management, reporting & communication, operations, use cases and detections. The survey also inquired about topics that are currently not part of the model: threat modelling and automation engineering and application of AI.

Reporting & metrics

Metrics can be used to measure performance in the SOC. In some cases, metrics and performance measurement are necessary to report on contractual agreements. A mature SOC will use metrics and KPIs to measure and improve its efficiency and quality. 64% of respondents indicate that there is no metrics program in place. The vast majority of these are either currently implementing a program or are planning to implement the program. For SOCs in the process of implementation or planning the implementation, the SOC-CMM metrics suite, and the 101 metrics presented there, may be a good starting point. The metrics suite provides both metrics and best practices for implementing a program.

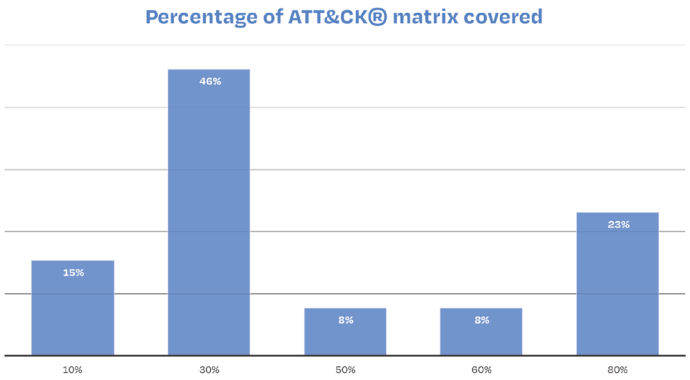
With only 3% of respondents indicating that the metrics program is implemented and optimised, it is clear that this is a topic that is still new and challenging to many SOCs.



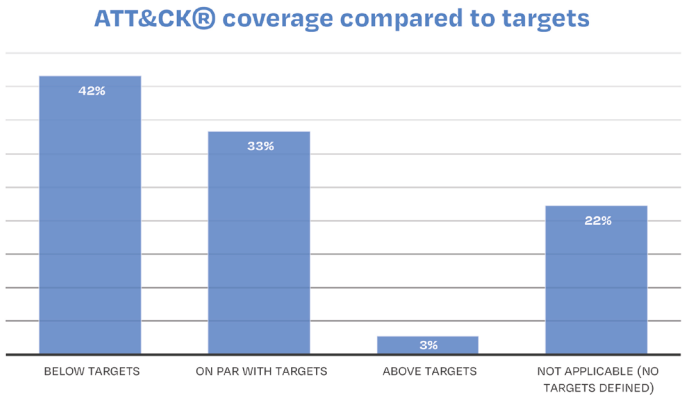
ATT&CK® coverage

Measuring and improving coverage against the MITRE ATT&CK® framework is an important way of quantifying detection capabilities. There are very few SOCs out there that do not yet leverage the possibilities that the ATT&CK® framework offers. With many products being able to generate ATT&CK®-based heatmaps, it has become easier to adopt the framework and measure progress.

Almost 50% of respondents indicated that they currently have coverage for roughly 30% of attack techniques. About 20% of respondents indicate coverage for 80% of the framework.



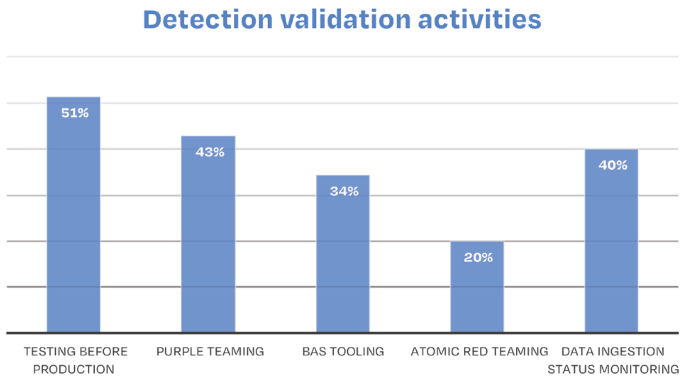
While the number in itself is an indication of detection completeness, it is also important to understand how this measures up against target values. By comparing this answer to the actual coverage scores, it can be concluded that SOCs that have no targets defined are found in the lower regions of scoring (10-30% of coverage). "On par with targets" is generally seen in SOCs with higher coverage scores (50-80% of coverage). This is an expected result, as lack of strategy (and targets) generally lead to lower scores. Having defined targets can be an enabler to direct growth opportunities but generally requires a more mature approach to detection completeness.



Detection validation

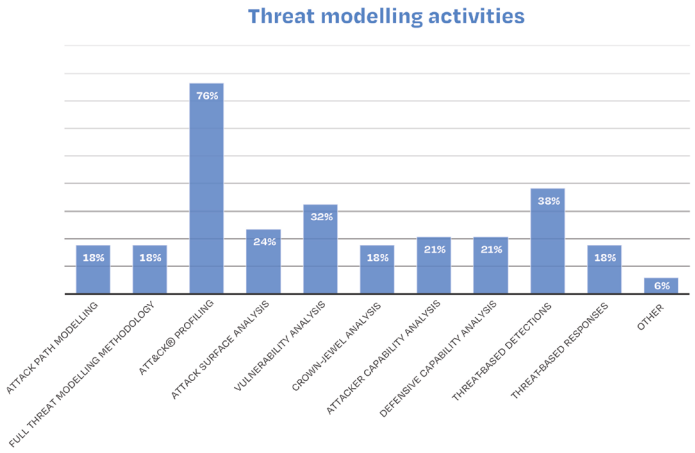
Detection validation is an important activity to ensure the accuracy of detection rules. Having inaccurate detection rules that do not fire can lead to a false sense of security, where coverage percentages seem to indicate a good posture, while in reality, incidents are missed. Common reasons for inaccurate rules vary from misconfiguration, to changes in data sources, incompleteness of data sources, or variations of attack that are not covered by the rule logic.

For validation purposes, most SOCs perform testing before moving to production. This is a good practice, but it must be noted that rules should also be tested after moving to production to ensure continued relevance and accuracy. Many SOCs indicate that they perform multiple activities to ensure detection quality, including manual activities (purple teaming), as well as fully automated activities (breach & attack simulation (BAS)) tooling. It must be noted that the majority of SOCs still rely on manual processes of testing and purple teaming, while does not scale well. Automated testing can be used to test almost the entire ruleset, resulting in a higher level of confidence across the entire detection capability.



Threat modelling

Threat modelling is currently not a part of the SOC-CMM model. However, many SOCs perform some type of threat modelling, although it may be named differently. The survey inquired about different threat modelling activities that SOCs may be using. Out of all possible answers, ATT&CK® profiling was the most common activity. In this activity, a SOC selects the most relevant ATT&CK® techniques. SOCs can base these on a combination of risks, threats, actor capabilities and existing controls. This results in an ATT&CK® profile or heatmap with most relevant techniques that can be used to prioritise detection efforts. Other slightly more common activities include vulnerability analysis and threat-based detections. All other activities are relatively uncommon, highlighting the relative immaturity of this topic within many SOCs.



Automation & AI

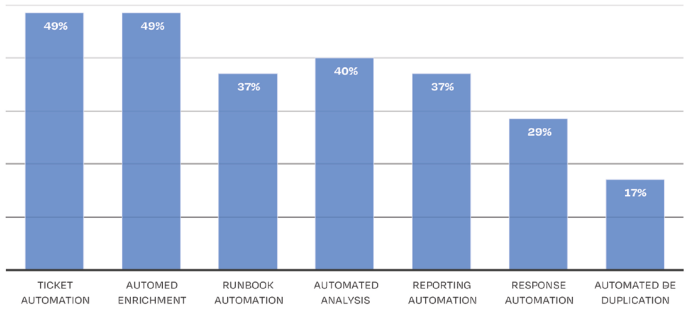
Automation and AI are currently not part of the process domain in SOC-CMM. The questions in the survey attempted to get a clearer view on application of AI and automation within the SOC.

Automation is an important topic for many SOCs. Automation can make security operations more efficient and more effective. Automation can also help in reducing required staffing levels, and making the job of analysts more interesting, thereby contributing to staff retainment.

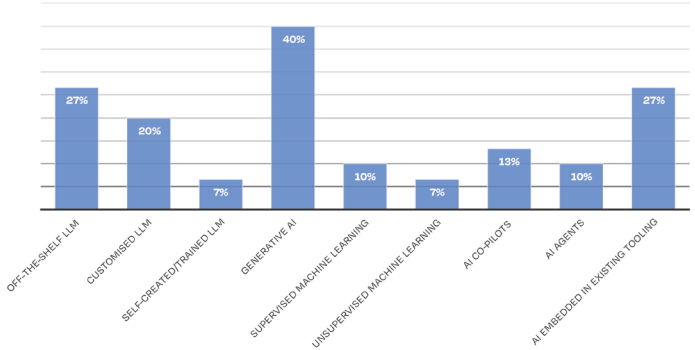
SOCs use automation for multiple purposes, the most common being ticket automation and automated enrichment. Runbook auto, automated analysis and reporting automation are also relatively common in SOCs. The impact of each of these types of automation for SOC efficiency varies. For SOCs, it can be helpful to divide automation into different categories: analysis automation, workflow automation, and response automation. By focusing on all categories, SOCs can apply a broader strategy to automation. Response automation is still relatively uncommon. As observed by the partner network, response automations are desired, but trust in the correctness of alerts, and concerns about (business) impact of response actions, are blocking to implementing such automated responses. SOCs can benefit from subdividing response actions per asset type and action (e.g. non-VIP personal laptop in the office network), so that risk assessment can take place. Low risk response actions can be automated.

Besides automation, Artificial Intelligence (AI) also provides SOCs with opportunities to become more effective. Currently, the landscape of AI in SOCs is still immature, with products in the innovation phase. The survey inquired about current usage of AI in the SOC. From the presented list, 40% of respondents indicate that they use generative AI within their SOC. From observations, usage of Gen AI for ticket and report generation, is becoming common practice in SOC. AI embedded in existing tooling and off-the-shelf LLMs (as opposed to customised or self-created LLMs) are also used in about 25% of responding SOCs. In general, it can be stated that application of AI in SOCs is currently limited. Over the next years, AI will likely move from the domain of early adopters to all SOCs.

Automation types used in SOCs



Application of AI types

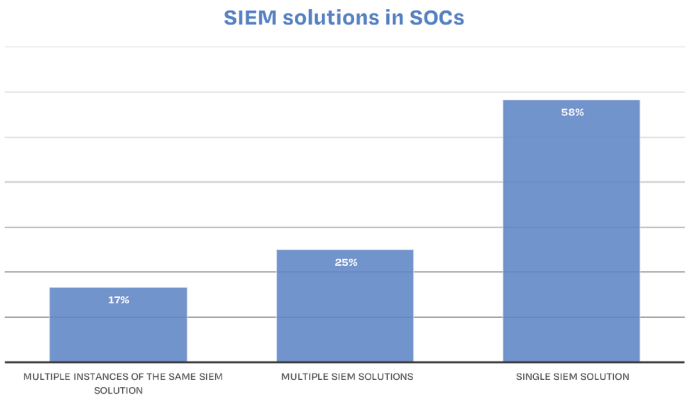


Technology domain

The technology domain of SOC-CMM has defined several technologies around monitoring, analysis, and response. The survey inquired about SIEM solutions, the single pane of glass and automation platform.

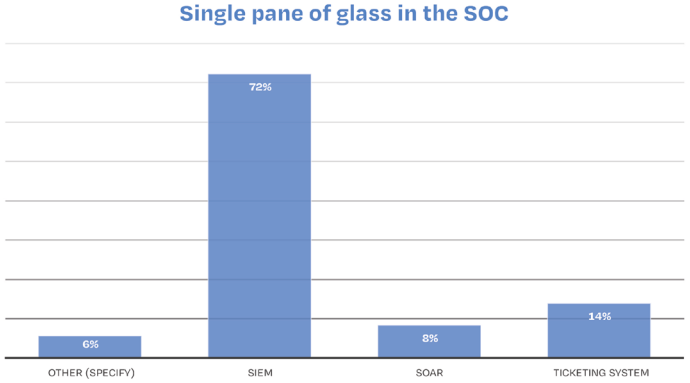
SIEM solutions

Despite having been declared dead time and time again, SIEM solutions still form the backbone of many SOC monitoring capabilities. Most SOCs rely on a single SIEM solution for all their monitoring needs. Some SOCs will have multiple instances of the same solution, while 25% of respondents indicate that they have multiple SIEM solutions. From observations in the support partner network, this is usually because there is an on-premises SIEM solution, and a different SIEM solution used for cloud-native security monitoring (see services section).



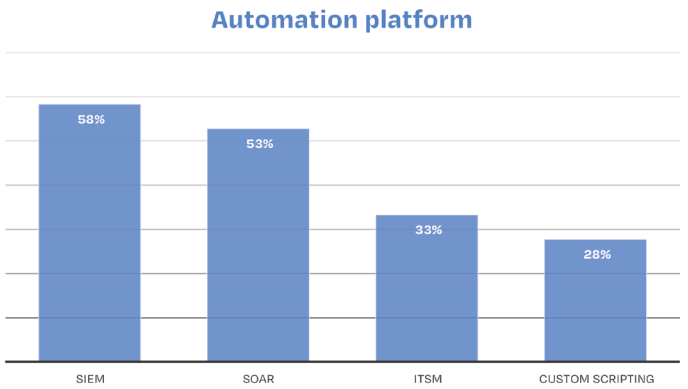
Single pane of glass

For most respondents, the SIEM solution is also the single pane of glass in which all relevant information is aggregated. Only a limited number of respondents have chosen a different technology. Having a single pane of glass is important for monitoring efficiency, so that analyst do not have to keep eyes on multiple screens and tools to perform their monitoring job. Besides these values, a security incident response platform was mentioned under other. This is an indication that the term 'single pane of glass' is subject to discussion. Such a platform could also be considered to be a sort of ticketing system or SOAR system.



Automation platform

Finally, the survey inquired about the automation platform used. For most respondents, this is either the SIEM or the SOAR. This represents the central role of SIEM systems for monitoring, as a single pane of glass, and for automation purposes. Since many SIEM systems also have SOAR functionality, the difference between SIEM and SOAR is becoming smaller. 28% of respondents are using custom scripting as a primary means for automation. While it provides a high level of flexibility, SOCs using custom scripting as a strategy should be concerned about manageability and continuity of knowledge to execute this strategy.

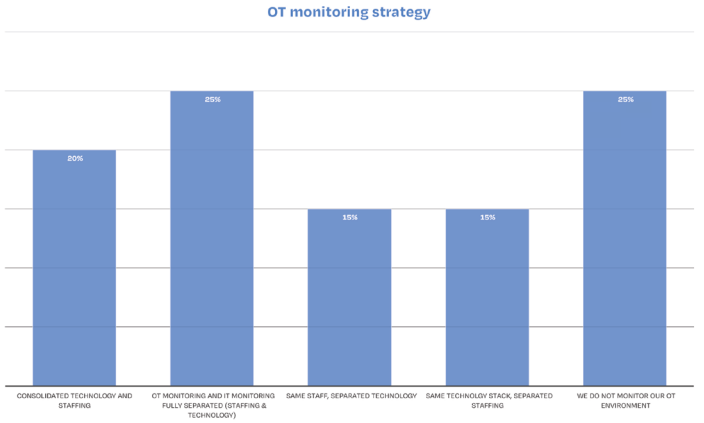


Services domain

The final domain that is part of the survey questions is the services domain. The topics in this section are OT monitoring and cloud monitoring.

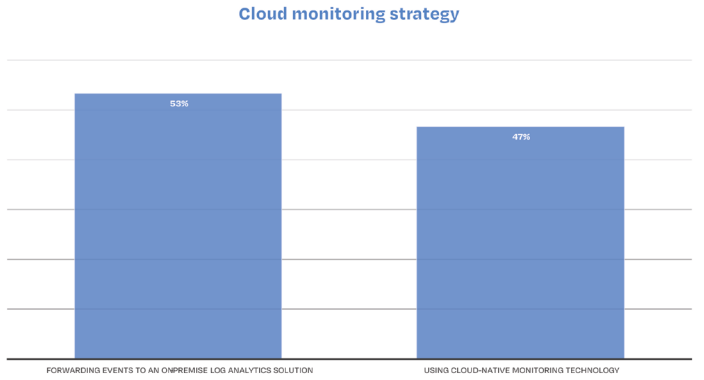
OT monitoring

Nearly 50% of respondents indicated that they have no OT environment. For those that do have an OT environment, there is great diversity in OT monitoring strategy. While OT and IT monitoring fully separated is the most common strategy, the differences with other implementations are not significant. It Nearly 25% of respondents indicate that the OT environment is not monitored at all. It must be noted that there are major differences between organisations in the significance of OT devices to their business.



Cloud monitoring

The survey also inquired about the cloud monitoring strategy used by the organisation. It is clear that there is no real preference for either using cloud-native monitoring technology or forwarding events to an on-premises log analytics solution (e.g. SIEM). This also means that over 50% of respondents are not using cloud-native monitoring capabilities but instead replicate these capabilities in their existing SIEM solution. For SOCs that have chosen this approach, it is important to keep up with the changes in functionality in the cloud environment, and the impact that this has on detection requirements and cloud visibility.



CHAPTER CONCLUSIONS

From the results presented in this chapter, it is clear that there are many differences between security operations centers and how they tackle challenges. There is no obvious single preference in topics like tiering, OT monitoring, cloud monitoring, automation platform, and detection validation strategy. For some topics, SOCs are more unified in their approach. For example, SIEM as a single pane of glass, analyst versus engineering ratio in favour of analysts, and ATT&CK® profiling as a threat modelling activity in the SOC are clearly preferred. Automation and AI are topics with great diversity. This supports observations in the support partner network that these are topics where many SOCs are still struggling to get it right. Lack of technology-agnostic best practices may contribute to this diversity.

CHAPTER 4

SOC certification

SOC certification

On October 31, 2024, the SOC-CMM certification program was launched, with a webinar session attended by attendees from 52 different countries. The SOC-CMM certification program represents the very first certification program for security operations centers that is based on an open standard and supported by a fully objective and accredited process. Interest for certification is increasing in various regions, for a number of reasons:

- Demonstrability of SOC quality and maturity is gaining attention in cybersecurity regulation, such as NIS2 and the Cyber Solidarity Act in the EU;
- Clients and prospects seek objective guidance in selecting a SOC service provider in an increasingly crowded market;
- Providers of SOC services are dealing with an increasingly competitive environment, where differentiation is becoming more important.

Existing generic security certifications, such as ISO27001 and SOC 2 type 2 provide assurance on information security within an organisation, but do not focus on security service delivery, or on the implementation of the maturity of SOC teams and services. Therefore, SOC-CMM provides a much higher level of assurance on the quality of SOC services.

SOC-CMM Certification levels

Through the certification program, SOCs can get certified on one of 3 levels:

Defined

A *defined* SOC represents a SOC that has implemented all elements of the SOC-CMM model and delivers services in a reliable and repeatable manner

Validated

A *validated* SOC represents a SOC that is able to deliver measurable services, and validates the correctness and quality of services

Risk-driven

A *risk-driven* SOC represents a SOC that is capable of aligning with customer / stakeholder risks and threats and uses this insight to deliver tailored SOC services

The right certification level for your SOC depends on ambitions, goals, organisational type, and the risk profile for your organisation or your clients (in case of an MSSP).

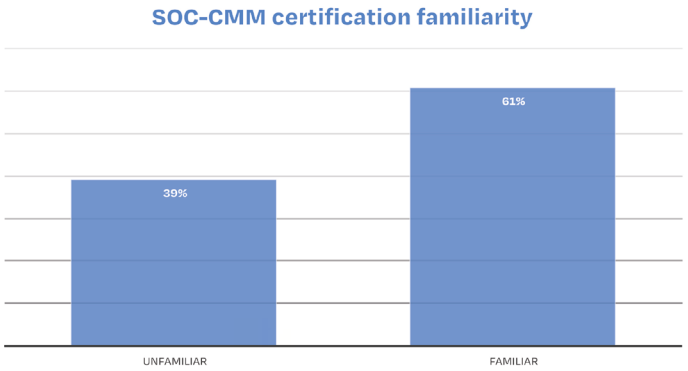
Currently, there are 8 SOCs certified. Of these SOCs, 5 are certified at the risk-driven level, 3 are certified at the validated level. At least 12 SOCs have formally initiated the certification preparation process to get certified as soon as possible.

Survey results

In the maturity survey, several questions were asked about the certification program.

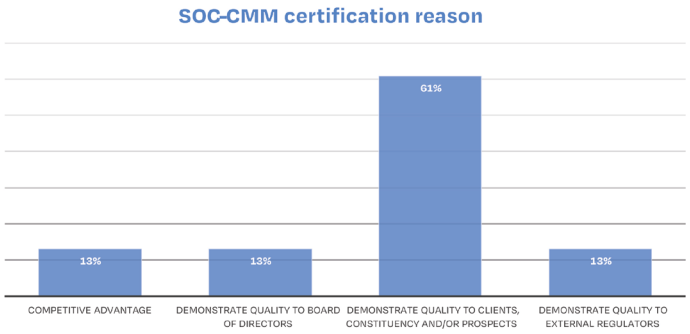
Familiarity with the certification program

From the survey, it is clear that most organisations are already familiar with the program. Given the number of questions received about the process over the last months, the documentation on the website was too extensive to get a quick grasp on the core of the program. This is the reason why a whitepaper on SOC-CMM certification was published, that presents a quick overview of the outlines, benefits, and processes in the certification program as well as a comparison to existing certifications.



Certification intention

When inquiring about the intent to get certified, 49% indicated that there was an intention to get the SOC certified. The reasons for getting the SOC certified vary, but the main reason is to demonstrate quality of service delivery to clients, constituency, and prospects. No specific differences were seen between in-house SOCs, MSSP SOCs and hybrid SOCs that expressed the wish to get certified in the survey, with the exception of competitive advantage, which is logically connected to MSSP SOCs. Additionally, no specific differences were seen between regions: certification intentions were observed in all represented regions. For sectors, a distinct observation was made that certification is mostly intended by MSSPs and hybrid and in-house security operations centers in critical sectors. Such sectors include finance, energy/utilities and governmental.



Certification timeline

During the launch of the certification program, a poll was held with the audience about the timeline for certification. From this poll, most SOCs indicated that they would like to be certified as soon as possible, or at least within 1 year. The survey results clearly indicate that this is still the preferred timeline for many SOCs, with 56% in total expressing the wish to get certified within 1 year at the latest. Whether or not this is realistic depends on the current state of the SOC. SOCs that have used the SOC-CMM assessment tool before, either as a self-assessment or a third-party assessment will find that the controls in the certification scheme are closely related to questions and topics in the assessment tool. The model used for certification is, for the most part, identical to the assessment model, albeit somewhat simplified in the technology and services domain. On average, SOCs that have a history with SOC-CMM and are in a relatively mature state, take about 3 months to get fully prepared. SOCs that are unfamiliar with SOC-CMM, or have a less mature state in general, may need to take up to 6 months for preparation. Engaging with a support partner that provides certification support can be beneficial in decreasing the preparation time required and increasing the chances of successfully passing the certification audit. From the survey results, about 30% of SOCs seeking certification plan to prepare using a SOC-CMM support partner; the majority plans to do preparations through an internal program.

Certification levels

During the launch webinar, another poll was held regarding the certification level. In the outcomes, most attendees indicated that risk-driven (the highest level) was the desired certification level. This outcome differs from the survey results, as most respondents indicated that they would like to aim for the validated level. The validated level is loosely associated with maturity level 4 in the SOC-CMM model, where quality assurance, measured service delivery, exercises, detection validation and continuity play an important role. While risk-driven does not represent a big step in terms of additional controls (the difference between validated and risk-driven is 17 controls), it does require a mature and capable threat intelligence practice, organisational risk-alignment, and a structured methodology for performing threat hunting investigations. These may be challenging topics for SOCs.

CHAPTER CONCLUSIONS

From the survey results, and the requests made to SOC-CMM, it is clear that there is an increasing demand for SOCs to get certified and demonstrate their maturity in an objective way. SOC-CMM, as an open standard, allows SOCs to transition from self-assessment to certification, with a support partner network in place to aid in preparations.

SOC-CMM developments 2025

SOC-CMM developments 2025

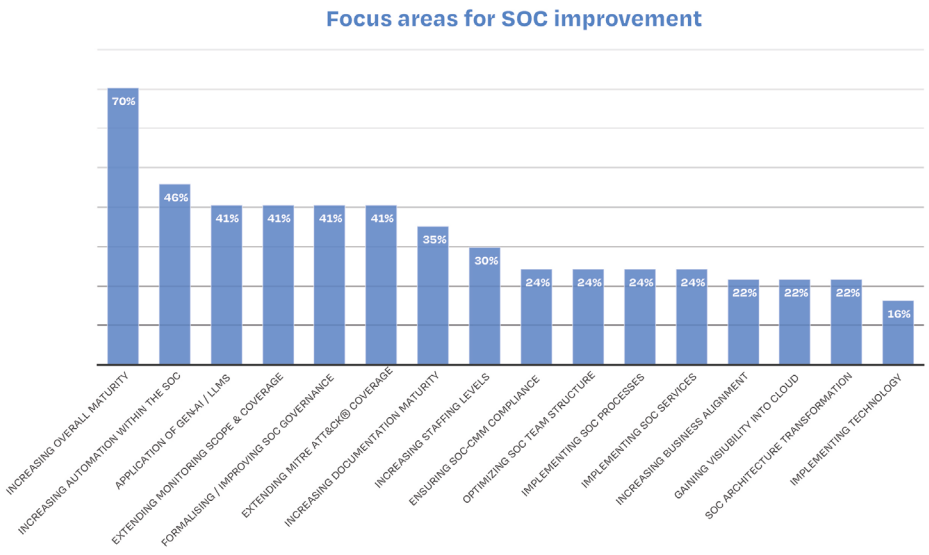
Part of the survey was reserved for questions on SOC-CMM itself: the format of the tooling, current usage and enhancement of SOC-CMM products and services, and improvements to the SOC-CMM model.

In the continuous development and improvement of the SOC-CMM model, there are several core principles that apply:

- The SOC-CMM model should be an accurate representation of a modern SOC;
- The SOC-CMM model follows established best practices, and does not dictate direction for SOCs;
- The SOC-CMM tooling should balance complexity with completeness.

It should also be noted that a model is a simplification and therefore will never cover all possible SOC topics and technologies.

SOC-CMM tries to align, wherever possible, with the needs of the SOC community. The following figure shows the focus areas for improvement within SOCs in 2025, which is used as input into improvement of SOC-CMM products and services.



SOC-CMM model updates

From the survey results, it is clear that there is demand for extending the model with additional tooling (such a CTI platforms, XDR, Breach & Attack Simulation and deception tooling). It is important to realise that not all of these tools are common practice in SOCs at the moment. Therefore, not all tools are eligible for inclusion into the SOC-CMM model.

The current SOC-CMM technology stack consists of SIEM/UEBA, EDR, NDR and SOAR. The basis for this is the traditional SOC visibility triad, augmented by the need for automation in SOCs. One of the improvements that will be made to the SOC-CMM model is moving away from any concrete product acronyms and using descriptions of tooling with examples of such tooling instead. The capabilities for an XDR platform can currently be evaluated by combining capabilities from SIEM/UEAB with SOAR capabilities. By using a descriptive name for a platform (such as: endpoint detection instead of EDR), the application of the SOC-CMM technology stack becomes more generic.

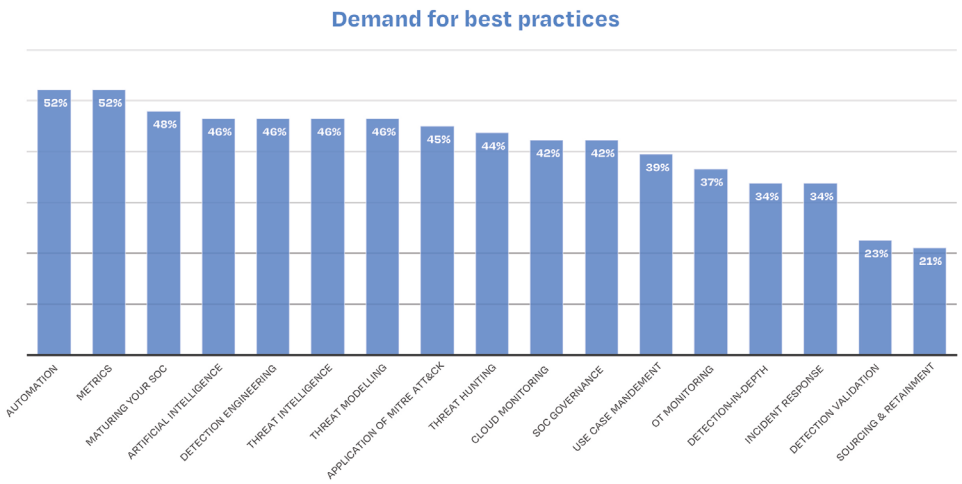
Besides additional tooling, additional processes are also in demand, with AI & automation, threat modelling and purple teaming all in demand. When combining this demand with the previously shown focus areas for improvement, and the demand for best practices (next section), AI and automation are clearly topics of great interest for SOCs. While automation is an established practice in many SOCs, AI (in particular LLMs and GenAI) are relatively new. Given the obvious demand, it is clear that this topic deserves a spot in the SOC-CMM model. Because best practices are lacking at the moment, this will be an aspect of the SOC-CMM model that will evolve further over the next years.

Additionally, the log management service has been considered a legacy service for few years. SOCs perform log management but rarely offer it as a service anymore. Therefore, capabilities from this service will be integrated or transferred to other parts of the model.

Finally, further simplification of the assessment tooling, to reduce the number of questions wherever possible, is planned for the next release, which is expected in Q3 of this year.

SOC-CMM products

When inquiring about SOC-CMM service and products enhancement, there was a clear demand for additional best practices, with over 50% of respondents indicating that this is an important topic to them. A follow-up question about those best practices yielded the following result:



SOC-CMM is planning to create a library of SOC best practices for these topics and populate this library over the next years with relevant information to the SOC community. Best practices will be aligned with existing SOC-CMM publications, such as the metrics suite and the assessment e-book. Besides best practices, whitepapers will also be published for selected topics where a more in-depth discussion is required.

SOC-CMM assessment tool format

Since its initial inception, the SOC-CMM assessment tool has been made available as a downloadable Excel file, without active content. From the survey results, this is still the preferred option for most users of the tool. However, demand for replacement of the Excel tool by either an online platform (similar to the SIM3 tool or the CIS Controls Self-assessment tool) or as a stand-alone application is increasing. SOC-CMM will look into the possibilities of alternative delivery methods for the tool.

SOC-CMM4CERT

The SOC-CMM product portfolio consists of 3 assessment tools:

- The SOC-CMM assessment tool (basic and advanced versions). Used for full capability and maturity assessment.
- The SOC-CMM screening tool. Used for quick evaluation of a SOC to identify obvious gaps and omissions.
- The SOC-CMM4CERT tool. Used to assess CERT/CSIRT teams for incident response maturity and capability.

The SOC-CMM4CERT tool differs from the SOC-CMM assessment tool, as it has a slightly different model. The tool itself has not been updated in a while and would need to be updated for continued relevance. Given the fact that other, more specific, methodologies exist for maturity evaluation in CSIRT teams, this tool will be discontinued. CSIRT teams that would like to continue evaluating their maturity with SOC-CMM, can do so by using the regular SOC-CMM assessment tooling, and selecting only relevant portions of the model for assessment. Further guidance for this will be provided.

Note: there is also a separate audit tool; this is used to SOC-CMM certification purposes and is therefore not considered part of the assessment suite.

CHAPTER CONCLUSIONS

With SOC-CMM becoming more commonly used throughout all regions, it is important to match the products and services with the expectations of the SOC community. Several modifications for the SOC-CMM model, especially in the process and technology domain, will be implemented to further align SOC-CMM with current SOC practices. The new model and assessment tool are expected to be released in Q3 of this year.

Besides the contents and the format of the tooling, best practices for SOCs are still hard to come by for many topics. SOC-CMM intends to address this gap through a library of best practices.

Partner insights

SUPPORT PARTNERS

CPX

SUPPORT PARTNER SINCE: NOVEMBER 2023

As CPX provides remote and on-prem SOC services to diverse clients, we observe trends for different sizes and types of organisations. Less mature organisations generally focus on improving visibility, while more mature organisations want to understand gaps in current SOC capabilities. Maturity and capability assessments as essential to identify gaps across technologies, processes and human resources. This is especially true in case of incidents. Recovery and lessons learned are an obvious priority, understanding gaps in SOC services is also important.

The importance of Threat Intelligence is increasing, as actionable intelligence in dynamic threat landscape can mean the difference between a major breach and a successfully contained incident.

For many teams, complexity and workload are the biggest challenges. SOCs attempt to battle these with automation and AI. More mature SOCs are using it to accelerate analysis and response, while others see it as a necessary step towards a more or less fully automated SOC.

Azeem Aleem
Executive Director - Cyber Resilience Services

Deloitte Netherlands

SUPPORT PARTNER SINCE: MARCH 2024

The past year has shown both changes and similarities in the challenges SOCs face and the solutions used. Modern technology stacks clearly enable faster initial SOC setups, but building a strong operational team remains challenging. For more mature organisations, we still see CTI, detection engineering and threat hunting as growth areas that are difficult to mature and sustain internally. Integrating OT monitoring or expanding its scope beyond a basic IDS approach has also been a recurring issue.

Technologies like SOAR and BAS are finally becoming mainstream, yet they remain underutilized as organisations grapple with the essential changes needed for automation- and test-driven detection. GenAI has been a recurring topic of interest, but few organisations effectively utilize it.

Addressing this requires strategic long-term planning aligned with senior stakeholders, stronger vendor management to better utilize existing technology, hands-on coaching for SOC personnel, and project-based initiatives to drive the necessary step change towards a futureproof SOC.

Bob van Kan
SOC Advisory lead

Kaspersky

SUPPORT PARTNER SINCE: FEBRUARY 2025

Despite overall strong results in people and technology management, we still observe below-expected maturity levels in SOC operations and services. A notable trend is the growing reliance of enterprise SOCs on detection content provided by solution vendors, with limited focus on self-driven detection engineering and use case management. This stands in contrast to MSSPs, who tend to maintain stronger in-house practices in these areas.

Interestingly, activities backed by built-in product functionality tend to show higher maturity levels. This suggests cybersecurity vendors not only influence SOC capabilities but also play a direct role in shaping maturity of security operations.

Regarding advanced services, most SOCs are gradually adopting best practices for threat intelligence and threat hunting. Encouragingly, SOC teams often share TI findings with other departments, be it in an ad-hoc manner, driven by individual initiative rather than formalized processes. AI adoption within SOCs primarily manifests as tools supporting SOC analysts (e.g., SOC Analyst advisors) and automating CTI analysis.

Roman Nazarov
Head of SOC Consulting Kaspersky

kaspersky

Northwave

SUPPORT PARTNER SINCE: NOVEMBER 2023

In the past years legislative pressure within the European Union regarding to cyber security has increased. Boardrooms are now actively involved in cyber risk management and question the state of the cyber security posture. We are observing an increase in SOCs wanting to actively improve the quality of their processes and services and showcase maturity toward stakeholders. For many SOCs in our client base, this has resulted in performing their first third-party SOC-CMM assessment. Third-party assessment provides an independent analysis of the current state and a roadmap with improvements which can be communicated towards stakeholders.

We observe a significant shift in interest towards the integration of artificial intelligence and machine learning within SOCs, enabling faster threat detection and response. The general shortage of good engineers and analysts makes transitioning to more automation difficult, resulting in a trend towards hybrid SOC models, combining in-house resources with managed security services and automation, providing flexibility and scalability.

Sjoerd Pellegrom
Sr. Cyber Risk & Strategy Consultant

NORTHWAVE CYBER SECURITY

Adarma

SUPPORT PARTNER SINCE: FEBRUARY 2024

The cybersecurity technology market is rapidly evolving, driven by increasing M&A activity and the growing influence of hyperscalers like Microsoft and Google. Significant consolidations, such as Cisco's acquisition of Splunk and QRadar's integration with Palo Alto Networks, highlight the trend toward unified security platforms.

While hyperscalers offer integrated, scalable solutions, dedicated providers like Splunk continue to deliver advanced and customisable features. CISOs face the challenge of balancing ease of integration, comprehensive capabilities, and cost-efficiency with the specialised flexibility that dedicated vendors can provide.

Working with an independent specialist like Adarma can help organisations optimise their security investments and manage the risks associated with platform migration.

Tim Davis
Principal consultant

ADARMA
TOGETHER WE'VE GOT THIS

Bionic Cyber

SUPPORT PARTNER SINCE: AUGUST 2024

Our work in the United States, the UK, and Europe has revealed a growing cyber capability gap between large, mature businesses and small to medium organisations. Spending slowdowns on staffing and advanced tooling disproportionately impacts smaller organisations who are already resource constrained.

That said, we perceive shrinking capability gaps between teams in North American and those in Europe, where increasingly onerous compliance requirements have driven investment in security operations.

Teams of all geographies and industries continue to struggle with SOC metrics and automation due to difficulties finding useful measures and the cost of building and maintaining automation.

Mark Orlando
Principal security consultant

BIONIC

BlueSec

SUPPORT PARTNER SINCE: SEPTEMBER 2024

We consistently observe SOCs facing growth challenges: talent shortages, lack of clear processes, difficulty in demonstrating value to leadership, and pressure of rapidly evolving cyber threats. SOCs seek not just technology, but a structured methodology to evaluate, benchmark, and mature SOC capabilities in a measurable way. The SOC-CMM framework allows us to provide an objective lens through which clients can identify strengths, uncover weaknesses, and build a tailored, actionable improvement roadmap.

Additionally, we see increasing demand for aligning SOC functions with regulatory requirements and business goals. As the SOC-CMM partner in Africa, we help our clients turn these challenges into opportunities, driving sustainable SOC growth and measurable resilience.

Imane BACHANE
Chief Executive Officer

BlueSec

Cross Mind Technology

SUPPORT PARTNER SINCE: APRIL 2025

Today, Security Operations Centers face an increasingly complex threat landscape. To keep pace, it is not enough to maintain what already works; evolution is necessary. Optimizing processes and incorporating technologies such as automation and artificial intelligence is no longer optional; it is essential.

However, to move forward with confidence, it is first necessary to understand where we stand. Assessing the current state of the service, identifying strengths and detecting areas for improvement allows for the development of a realistic plan aligned with both the organisation's strategic vision and business needs. This is key to effectively addressing core challenges and fostering continuous improvement.

Roberto Carlos Pérez González
Principal Cybersecurity Consultant

Cross Mind
Technology

CyberACI

SUPPORT PARTNER SINCE: JUNE 2024

Organisations increasingly prefer hybrid SOCs, combining internal capabilities with MSSPs to maximize efficiency and expertise. This hybrid model addresses ongoing challenges posed by staffing shortages, as retaining qualified cybersecurity professionals remains difficult. To mitigate these gaps, we also engage with SOCs actively explore AI-driven automation for routine operational tasks.

While AI promises significant workload reduction and improved operational effectiveness, many organisations still struggle to clearly understand AI's true capabilities and limitations. This uncertainty complicates developing effective strategies that combine AI automation with essential human oversight.

Asif Safdary
Strategic SOC advisor

Datasec

SUPPORT PARTNER SINCE: NOVEMBER 2023

The current global dynamic and multi-tiered threat landscape requires organisations to protect themselves from regionalized opportunistic frauds, global internet DDoS outages, and advanced persistent threats. This creates a distinct risk model for each organisation, that requires the appropriate SOC services and implementation strategy. We observe that these challenges increase the need for SOC Advisory, Assessments and Certification process, guided and supported by SOC-CMM tools and standards. This helps organisations to achieve the best outcome with their current resources and guides them to next-level Cyber SOC capabilities supporting their budgeting, operational and go-to marketing & selling-up strategy to internal and external customers.

Bruno Guerreiro
Managed Security Services and SOC Chief Advisor

GroupIB

SUPPORT PARTNER SINCE: JUNE 2024

Our engagements reveal an accelerating shift from reactive security operations to a proactive approach, prioritizing Threat Intelligence and Threat Hunting. Instead of merely ingesting IOCs or conducting IOC scans, SOCs are increasingly focusing on the top three layers of the Pyramid of Pain to enhance and mature threat mitigation.

SOAR, as a standalone system, is becoming obsolete - clients are opting for XDR and other tools to address operational demands more effectively. Demand for SOC-CMM certification is surging, particularly among MSSPs seeking to benchmark and demonstrate the effectiveness of their security services

Alexander Asmolov
Global Head of Cyberdefense Consulting

HelpAG

SUPPORT PARTNER SINCE: NOVEMBER 2023

Across the GCC region, we observed a trend in local regulatory requirements that aligns closely with SOC-CMM. A recurring challenge in our engagements is the absence of documented SOC charters, which hinders clear operational mandates. To enhance SOC effectiveness and resilience, organisations should focus on strengthening knowledge management and implementing upskilling programs to ensure consistent service delivery.

Smaller organisations, in particular, exhibit maturity gaps in operational and facilities processes. Additionally, there is a pressing need for improved incident response playbooks, streamlined vulnerability management workflows, and enhanced threat detection capabilities. Addressing these areas will significantly improve the overall maturity and efficiency of SOC operations.

Talal Wazani
Head of Cyber Trust Advisory

iT.eam

SUPPORT PARTNER SINCE: NOVEMBER 2023

Analyzing our clients' demands, we have observed a strong interest in automation and a significant curiosity about how artificial intelligence is being applied in SOC operations. A constant challenge is: how to build automations when clients' processes are not yet well-defined or mature?

We have focused our efforts on internal processes and, among other projects, are maximizing automation in the alert triage and enrichment stage to optimize our analysts' work. We believe this effort will allow us to handle the increase in clients and growing demand more efficiently, enabling us to deliver more with existing resources.

Paulo Nunes
Head of Security Operations

IT Security C&T

SUPPORT PARTNER SINCE: JANUARY 2025

A major issue is the lack of well-documented processes, causing inconsistencies and impeding the SOC's efficiency. Resource constraints and insufficient automation also make it difficult to manage growing alert volumes while aligning with broader organisational goals. Poor integration between incident management and business functions results in delays and miscommunication.

Additionally, detection rules, both traditional and AI-powered, are often poorly tuned, leading to missed threats and false positives. The adoption of GenAI, LLMs, and other emerging technologies offers new opportunities, but SOCs must address integration, data quality, and model complexity to remain resilient. Continuous improvements in training, process optimization, and technology integration are essential to enhance SOC effectiveness and resilience.

Aws Al-Badawi
Senior Cyber Security Consultant and Trainer

Lemonshark

SUPPORT PARTNER SINCE: FEBRUARY 2025

Over the past year, the overall demand for SOC solutions has grown.

The incorporation of AI into SOC platforms has increased. This helps the SOC teams to respond faster to threats their organisation is facing.

Stricter regulations in Europe have raised the need for better security monitoring and reporting. SOC solutions play a crucial role in helping organisations meet these compliance standards, also when it comes to their chain of suppliers and customers.

These developments highlight a robust market for SOC services, presenting Lemonshark with opportunities to engage in various roles, from implementing SOC-CMM to providing advice tailored for customers.

Erik Heskes
Senior Cyber Security Consultant

LEMON SHARK CYBERSECURITY

Montance®

SUPPORT PARTNER SINCE: NOVEMBER 2023

Based on assessments, the SANS SOC Survey, and consulting engagements, several emerging trends are observed.

Emerging trends include: the obvious mandate to utilize, implement, and defend AI. This includes generative (GPT), machine learning (ML), and automation. As documented in the SOC Survey, SOC dissatisfaction with AI in all aspects is high. Another emerging trend is the inclination to try to stash everything in the SIEM, and the understandable resulting questioning from the organisation, "What value do we derive from paying to store these logs?" The SOC use case development and detection engineering should establish correct data collection, but that is too complicated for most SOCs to do.

Chris Crowley
author, consultant, instructor

Montance®

Nettles

SUPPORT PARTNER SINCE: MARCH 2024

Over the last year, we have seen many SOCs continue to face challenges that significantly impact their efficiency. One of the most troubling areas – besides senior analyst retention issues that cause knowledge drain and over reliance on junior staff – is defaulting to "out-of-the-box" analytics and rules and failing to align detection strategies with customer-specific threat models. This often leads to generic, low-context alerts.

Addressing these issues requires a shift toward more targeted detection frameworks. Encouragingly, progress has been made in this area with increased adoption of threat modelling, particularly using MITRE ATT&CK, to refine targeting of detection engineering activities.

Jan Kopriva
Cyber security consultant and trainer

NETTLES CONSULTING

NVISO

SUPPORT PARTNER SINCE: JANUARY 2024

As a leading European cybersecurity service provider, specializing in SOC, MDR and consulting services, we serve a variety of sectors including finance, government and manufacturing and have addressed key challenges such as alert fatigue and rapid incident response. Solid SOC architecture, and enhanced threat detection and incident response capabilities are essential to address these challenges.

A common observation is that SOCs typically have a strong focus on solutions, yet technology is only one piece of the puzzle that makes a successful SOC. Leveraging the SOC-CMM framework, we work with our customers to achieve a solid roadmap together that ensures a capable, mature and future-proof SOC across the board.

Koen Vanhees
Security Operations Engineering
Global Solution Lead

nviso

Scybers

SUPPORT PARTNER SINCE: APRIL 2025

The modern SOC is undergoing a profound shift: from being a reactive, alert-centric function to becoming a strategic, AI-powered, threat-informed defense advisory unit. By embracing cloud-native SIEM platforms, deeper threat intelligence integration, and proactive threat hunting, proactive SOC leaders are delivering actionable insights that drive organisational resilience and address growing executive concerns.

Coupling technical capabilities with CISO-level advisory ensures that security becomes tightly woven into overall business strategy, transforming the SOC into a critical capability for sustainable and secure growth.

Kugan Kulothungan
CEO Scybers Inc.

SCYBERS

SimplifyNow

SUPPORT PARTNER SINCE: OCTOBER 2024

We've observed SOCs are increasingly shaped by artificial intelligence, automation, and real-time analytics, reshaping how threats are detected and managed. While these innovations streamline security workflows, they also introduce complexity in hybrid and multi-cloud environments, placing additional demands on specialized personnel.

Organisations are adopting Zero Trust approaches and enhancing threat intelligence integration to proactively address evolving cyber risks, including advanced ransomware and AI-driven attacks.

Growing regulatory expectations and privacy requirements further influence operational strategies. Effective SOCs now rely heavily on balancing automated systems with human judgment, strengthening their ability to quickly respond to sophisticated threats in a rapidly changing cybersecurity landscape.

Victor Fleuren
Cyber Security Consultant

SIMPLIFYNOW

SopraSteria

SUPPORT PARTNER SINCE: JANUARY 2024

In the current SOC market, companies often struggle to maintain their SOC at the required quality level, leading them to outsource SOC services to specialized firms. This trend is driven by a staff shortage and the need to focus on core business activities.

Additionally, the market-wide shortage of skilled personnel forces companies to make strategic choices. SOC specialists are increasingly opting for specialized employers to be part of a community and further develop their skills.

The SOC market is expanding rapidly due to the complexity of cyber threats and the need for robust security measures across industries.

Helmer Berkhoff
Practice Lead Security Operations & IAM

Thales

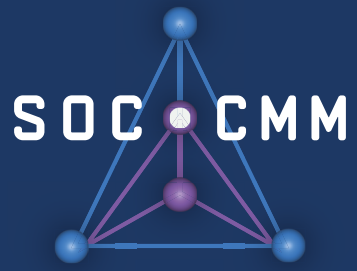
SUPPORT PARTNER SINCE: OCTOBER 2024

Throughout our client engagements, SOC maturity is crucial for advancing business understanding, people, processes, and technology within IT, OT, and embedded system security. It ensures robust and continued cybersecurity resilience through continuous improvement, maturity growth, accurate measuring, and integration of AI and advanced tools.

Current trends highlight increased use of AI-driven analytics, automation, and threat intelligence to counter sophisticated threats. MSSPs provide expertise to help SOCs tackle challenges like analyst retention and effective AI adoption.

A mature SOC enhances operational quality and strategically aligns with future business and security demands, ensuring resilience and continuous improvement.

Michael Cormack
Strategic SOC advisor
& SOC Advisory Manager


SOC CMM