Defining and operationalising a SOC Target Operating Model using the SOC-CMM

1 Introduction

Security operations can be hectic. Running the SOC business includes dealing with continuous and ever-increasing event and alert flows, managing incidents, reducing false positives, and analysing and responding to threats. This is all in a day's work. However, balancing operational activities with continuous improvement and managing SOC expectations and ambitions can be challenging.

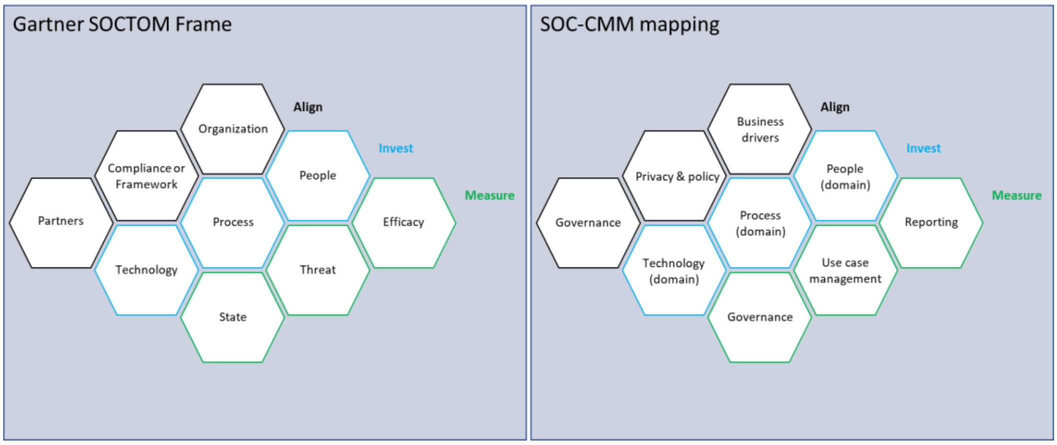
In 2020, Gartner released a research paper on creating a SOC target operating model: Create a SOC Target Operating Model to Drive Success [[1]]. This is an excellent piece of work that outlines the importance of creating a Target Operating Model (TOM) to provide strategic direction for the SOC. This strategic direction is crucial for obtaining long-term goals, supported by the right level of management within the organisation. This whitepaper explains how to use the SOC-CMM to define and operationalise your target operating model, introduces the SOC-CMM SOCTOM tool, and provides best practices and guidance for defining your SOCTOM.

1.1 Mapping the Gartner framework to SOC-CMM

To understand the relationship between the Gartner paper and the SOC-CMM, a brief introduction of the Gartner framework is required. The Gartner paper presents a framework of SOCTOM elements in the following areas:

- **Align**, which includes organization, compliance or framework and partners
- **Invest**, which includes people, process, and technology
- **Measure**, which includes state, threat, and efficacy

These elements can be mapped to aspects of the SOC-CMM model. Organisational alignment is found as 'business drivers' in the SOC-CMM, compliance and framework to 'privacy & policy', partners to 'governance', etc. The match is not 100%, but sufficiently solid. The following figure shows the mapping of the Gartner SOCTOM Framework to SOC-CMM.



[1] https://www.gartner.com/en/documents/3979602

1.2 Differences

One of the biggest differences is in the 'Threat' element from the Gartner model. It is explained as: "*Threat modeling and continuously measuring threat exposure drive risk identification, talent needs, process improvement and pertinent tool selection*". While the current version of the SOC-CMM does include measuring use cases, data source visibility and coverage to Mitre ATT&CK© to determine the threat detection capability, this is different from actual threat modelling. Threat modelling will be introduced in a later version of the SOC-CMM. There is an article on practical threat modelling for SOCs [[2]], which can provide an approach to start with threat modelling if you do not have one already.

Another major difference Gartner SOCTOM Framework and a SOCTOM based on the SOC-CMM is the level of detail. The SOC-CMM is designed as a self-assessment tool that provides a granular view of the state of your security operations. Measuring that state is part of the Gartner framework, so will fit right in there.

Using the SOC-CMM to build your target operating model is beneficial because it allows you to measure the current state, define a target state and measure progress towards that state within the same framework.

2 Defining the SOCTOM

The SOCTOM represents the desired state that the SOC needs to move toward. This target state is the concrete definition of a SOC that is in line with its mission and ambitions. The target state sets a direction for the SOC and helps to move forward in a structured way.

The following steps need to be taken to define the SOCTOM:

1. Determine the SOC goals, success criteria and ambition
2. Determine the SOCTOM horizon
3. Determine the current state
4. Define the target state
5. Approve the target state

2.1 Determine the SOC goals, success criteria and ambition

The journey towards a target state for your SOC starts with goals and ambitions. It is vital to have a clear understanding and vision of where the SOC needs to go. This vision must be aligned with organisational goals. Investment in a target operating model requires support from senior management, so alignment with organisational goals is critical. If your SOC has created and maintained a SOC charter, the ambition, goals, and success criteria may already have been defined and approved at the senior level. This will help to speed up the SOCTOM definition process.

2.2 Determine the SOCTOM horizon

The horizon of the SOCTOM is the target date (defined as year) in which the SOC should have achieved its target state. Determining the SOCTOM horizon is relevant, because it helps to define the roadmap and priorities for the SOC, as well as the pace that is required for progressing to the target state. Note that, like any improvement initiative, improvement requires resources. The pace of improvement determines how many resources are required. Also note that running a SOC at the target operating model itself may require more resources than currently available in the SOC. Proper planning of resources is critical for a successful path to a target state and maintaining that state. It is also possible to define a single target state with multiple horizons (stages). In this case, it should be clear what state is required at what moment in time. This is a more complex approach but helps to define the roadmap with more accuracy.

[2] https://www.linkedin.com/pulse/practical-threat-modelling-socs-rob-van-os/

2.3 Determine the current state

With the goals and ambition as well as the SOCTOM horizon determine, the next step is to determine the current state of the SOC. This current state will serve as a baseline and starting point for the SOC. IT can also be used to show progress of the SOC towards the target state to relevant stakeholders. If you are already using the SOC-CMM to assess your SOC, the latest assessment (provided it is not too old) can serve as a starting point. If a SOC-CMM assessment is not available or not current anymore, a *quickscan* can be done, which is sufficient for this purpose. A *quickscan* is an informal way of determining the current state of a SOC and can be conducted by a single person who is highly knowledgeable about all domains in the SOC and may be verified by peers. The SOCTOM tool (discussed in chapter 4) provides the outline for the *quickscan*.

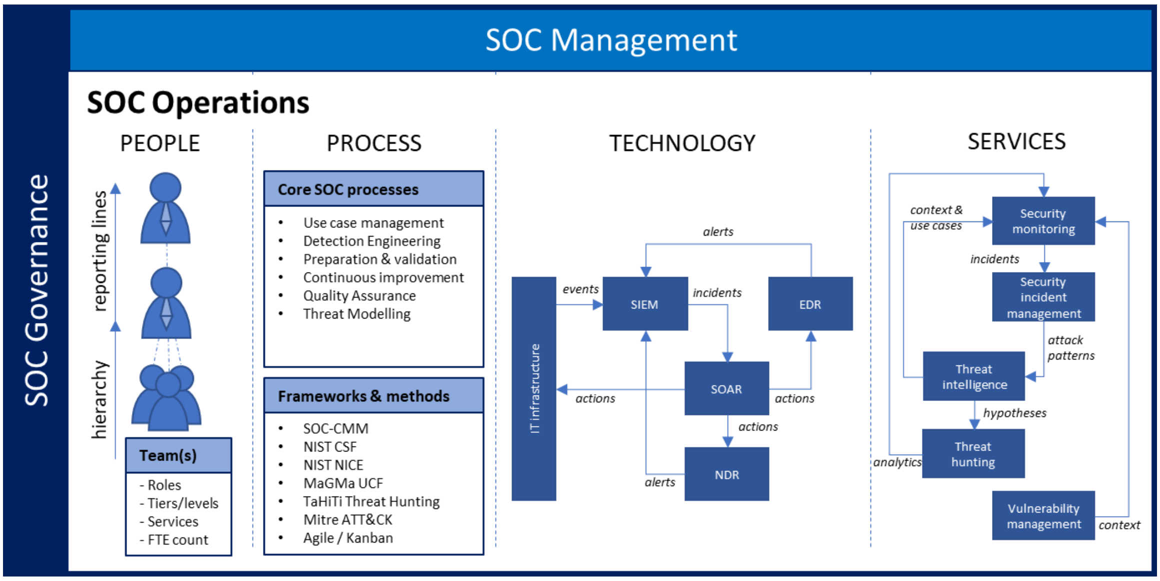
2.4 Define the target state

The next step in the process is the actual definition of the target operating model. In this step, the target state on the defined horizon or horizons is made concrete. The target state can be defined in terms of maturity levels, specific capabilities, documentation levels, FTE counts, etc. All these elements are part of the SOCTOM tool. The level of detail for each of these elements depends on the current state and the horizon. For SOCTOM elements with a longer horizon, having a detailed target state makes little sense as things are likely to change along the way. For those elements that need to be operationalised in the near future, much more detail is required.

2.5 Approve the target state

Once the target state has been defined, it should be approved by senior management. This approval will ensure that the initiative is backed at the right level. It will also ensure that investments that need to be in process improvement and any additional technology are understood. Note that a business case will likely be needed to formally outline costs and benefits.

A visualisation may help to communicate the results of the SOCTOM to relevant stakeholders within the organisation. An example visualisation is shown in the figure below. This is a high-level visualisation that only shows the major outlines of the SOC, which should be sufficient for communication purposes.



3 Operationalizing the SOCTOM

Now that the target operating model has been defined, the next major step is to operationalise the SOCTOM. The SOCTOM consists of many elements, so operationalising it should be an iterative approach rather than a big-bang initiative. For this iterative approach, it is important to have a structured way of implementing elements of the SOCTOM that takes interdependencies and logical order of implementation into account.

The following steps need to be taken to operationalize the SOCTOM:

1. Determine the gap
2. Build the backlog
3. Embed the TOM backlog in a continuous improvement process
4. Measure and adapt

3.1 Determine the gap

In the previous phase, both the current and target operating models were defined. The first thing to do is to perform a gap analysis. The gap analysis should focus on defining concretely what is required to move from the current state to the target state for a particular element.

3.2 Build the backlog

With the gap analysis completed, the next step is to take its output and convert it into an improvement backlog. The backlog should be structured in a tree structure using epics, features, and tasks so that it becomes a logical grouping of elements. Common elements that may need to go on the backlog are:

- **Business case** for the investments required for the target state
- **SOC charter** that outlines mission, vision, strategy, goals, success criteria, etc.
- **Extended RACI** that defines different activities and ownership of those activities. The RACI also outlines how the SOC interacts with other parts of the organisations and/or the SOC customers
- **Additional reports and / or dashboards** to provide insight into security operations and improvements
- **Sourcing strategy** to attract and retain security talent
- **Process descriptions** for processes like use case management and threat hunting
- **Procedures** for efficient and effective security operations
- **Technical documentation** that supports knowledge management in the technology domain
- **Strategies**, such as cost management strategy, assessment strategy, continuous improvement strategy, quality assurance strategy, etc.
- **Architecture diagrams**, such as the service architecture, technology architecture, etc.
- **Policies** that are required for SOC operations
- **Role model** that describes the roles, staffing levels and hierarchy in the target state
- **Role descriptions** for the roles defined in the role model

Another important thing for the success of the improvement program is clearly defining the ownership of the improvement backlog. The backlog owner manages and reports on progress, manages the improvement timeline and identifies and escalates blocking issues. The owner of the improvement backlog can be the SOC manager, or someone delegated by the SOC manager to take on the responsibility.

3.3 Embed the TOM backlog in a continuous improvement process

With the backlog completed and structured in a logical way and the ownership of the backlog clearly defined, the next step is to start operationalising the backlog in an iterative and agile approach. This can best be done by embedding the SOCTOM backlog into an existing continuous improvement process. If no such approach exists, one should be implemented. The continuous improvement approach deals with both the SOCTOM items intended to move towards the desired state, as well as other improvement initiatives. Careful balancing resources for operations, general improvement and SOCTOM improvement to ensure that the team can function effectively without being overloaded. As indicated, additional (temporary) resources are required in the journey towards the target operating state.

3.4 Measure and adapt

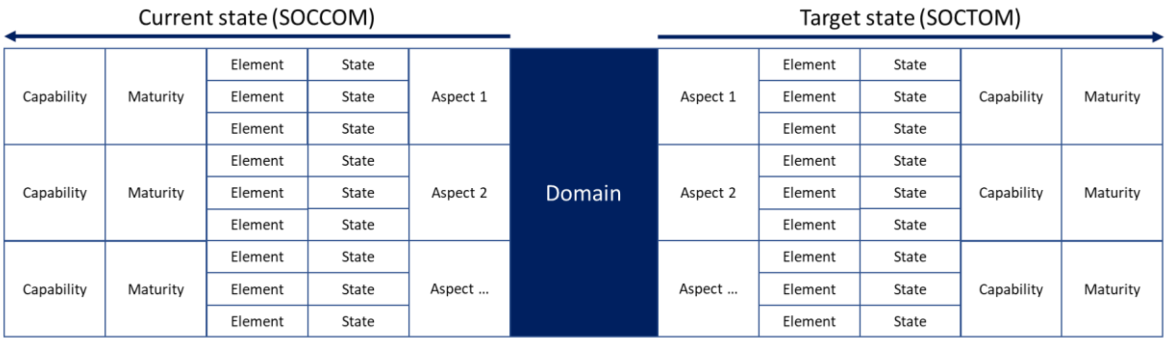
The last step to take in realisation of the SOCTOM is measure and adapt. With the long horizon of the SOCTOM, it makes sense to regularly track progress and check whether the SOC is still moving in the right direction. Of course, the backlog, and especially the tasks that have already been resolved are proof that the SOC is working to move towards the desired state. However, regularly assessing the state of the SOC can help to verify that the activities have led to the desired results. Such assessments can be done in the form of a SOC-CMM assessment, as either a full assessment or a *quickscan*. The results of an assessment may be that additional backlog items are required, or existing backlog items should be modified.

Besides assessing the current state, it also makes sense to regularly check whether the target state is still the desired state. There may have been changes that require modification of the target operating model. This is especially true when the horizon of the SOCTOM is set to several years. If changes that affect the target state have taken place, the target operating model must be updated, a focused gap analysis must be executed, and an update of the backlog is required.

4 Using the SOC-CMM SOCTOM tool

On the SOC-CMM webpage, the SOCTOM tool is available for download [3]. This SOCTOM tool provides a structured means to define both the current and target operating model in the desired level of detail. The information in this tool can serve as the basis for the gap analysis described in the previous chapter. The tool is a summary of the SOC-CMM and contains all elements of the SOC-CMM that are relevant to define a target operating model.

The SOCTOM tool is structured as follows: centrally, the SOC-CMM **domains** and **aspects** are positioned. These are the domains and aspects that are part of the SOC-CMM model. For each aspect, several **elements** are defined, which summarize the aspect. For each element, the **current state** and the **target state** can be defined. The current state is shown on the left, the target state is shown on the right. Current and target maturity and capability can be scored per aspect, to keep it aligned with SOC-CMM scoring and provide the ability to use SOC-CMM scores directly in the SOCTOM tool.



Current state (SOCCOM)

Target state (SOCTOM)

Capability	Maturity	Element	State	Aspect 1	Domain	Aspect 1	Element	State	Capability	Maturity
		Element	State				Element	State		
		Element	State				Element	State		
Capability	Maturity	Element	State	Aspect 2		Aspect 2	Element	State	Capability	Maturity
		Element	State				Element	State		
		Element	State				Element	State		
Capability	Maturity	Element	State	Aspect ...		Aspect ...	Element	State	Capability	Maturity
		Element	State				Element	State		
		Element	State				Element	State		

Note that not all rows will make sense in all situations. Rows can either be deleted or marked as 'not applicable' with the explanation why this is not the case. The latter is recommended in a more formal organisation, as it provides a more auditable result. Of course, rows can also be added if certain

[3] https://www.soc-cmm.com/downloads/latest/

relevant elements of the SOC are not captured in the tool. As indicated, capability and maturity targets can be set as well. This can make sense if there are capability and maturity requirements for the SOC. It can also make sense if a certain level of maturity matches the ambitions and targets for the SOC. Note that achieving a certain maturity level itself should not be the SOCs ambition. Instead, the SOCs required maturity level should be derived from its ambition.

The current and target state can be defined in high-level terms as well as a detailed state. Providing more detail for certain elements makes sense if the element will be implemented soon. Choosing the right level of detail for each element will help in defining a SOCTOM that is both capable of providing the right direction for the SOC as well as providing concrete definitions and flexibility. The SOCTOM horizon or stages should be used to determine the required level of detail.

5 Conclusion

Defining a target operating model for your SOC is a powerful way of providing strategic direction for the SOC. Starting out with the strategic goals of the SOC, a target state for the SOC can be defined in the level of granularity that is fitting for the SOCTOM horizon. Comparing the target operating model with the current state helps to identify areas that need to be implemented or improved on and can serve as the foundation of an improvement roadmap.

The SOC-CMM SOCTOM tool provides a concrete method to define the SOCTOM. Because the tool is structured using the SOC-CMM, but in a simplified (and extended) form, it is aligned with maturity measurement and improvement initiatives within the SOC. With the SOCTOM tool and frequently assessing the SOC using the SOC-CMM, SOCs can both define the target state and move towards that state in a structured and measurable fashion.

5.1 Best Practices

To conclude, here is a summary of best practices for defining a SOCTOM:

- Start out with the SOC **ambition and goals**. Theses provide a strategic viewpoint, from which the target state should be derived.
- **Align** the SOCTOM with business goals and have it formally **approved**. This will ensure management commitment for the target SOC state and the improvement initiative.
- Accurately determine the **horizon** for the SOCTOM. Note that the further in the future, the less detailed the SOCTOM should be.
- Take an **agile** approach. As we know, the only constant is change. Threats change, technology changes, businesses change. Thus, setting the target state and moving forward regardless of change will lead to the SOC moving in an undesired direction. So, take an agile approach to the TOM and adapt where required.
- Use the SOC-CMM SOCTOM **tool**, because it provides a structured approach based on the SOC-CMM and can thus consolidate SOC maturity assessment with the SOC target operating model.
- Defining a target operating model without defining the current operating model makes less sense, as the creation of an improvement roadmap requires a proper **gap analysis**.
- Choose the right level of **detail** for the definition of the SOCTOM. The level of detail in the elements of the SOCTOM depends on the horizon for implementation of those elements.