SOC-CMM

Measuring Capability Maturity in Security Operations Centers

Introduction

In many organizations, Security Operations Centers (SOCs) are center of expertise where knowledge and skills regarding cyber security are aggregated. The SOC is where log information collected throughout the enterprise is gathered, processed and analyzed by skilled individuals to find indicators of cyber threats in the infrastructure. Thus, the SOC adds value to business by increasing the resilience of the organization against cyber threats and minimizing damage resulting from cyber attacks.

With this central role in cyber defense comes responsibility. Responsibility to function effectively and efficiently and to stop cyber threats before they have a disruptive effect on the business. This is where capability maturity measurement comes into play. Capability maturity measurement is a SOC management tool that can be used to determine strengths and weaknesses of the SOC. Furthermore, it provides a means for measuring growth of the SOC, thereby demonstrating the return on investment in the SOC. The SOC-CMM is a self-assessment tool for capability maturity measurement that enables SOCs to measure and grow, thus providing the greatest possible added value to the business.

Capability Maturity

The SOC-CMM uses capability maturity loosely based on the CMMi created by Carnegie Mellon. Below is an overview and brief description of the SOC-CMM capability and maturity levels:

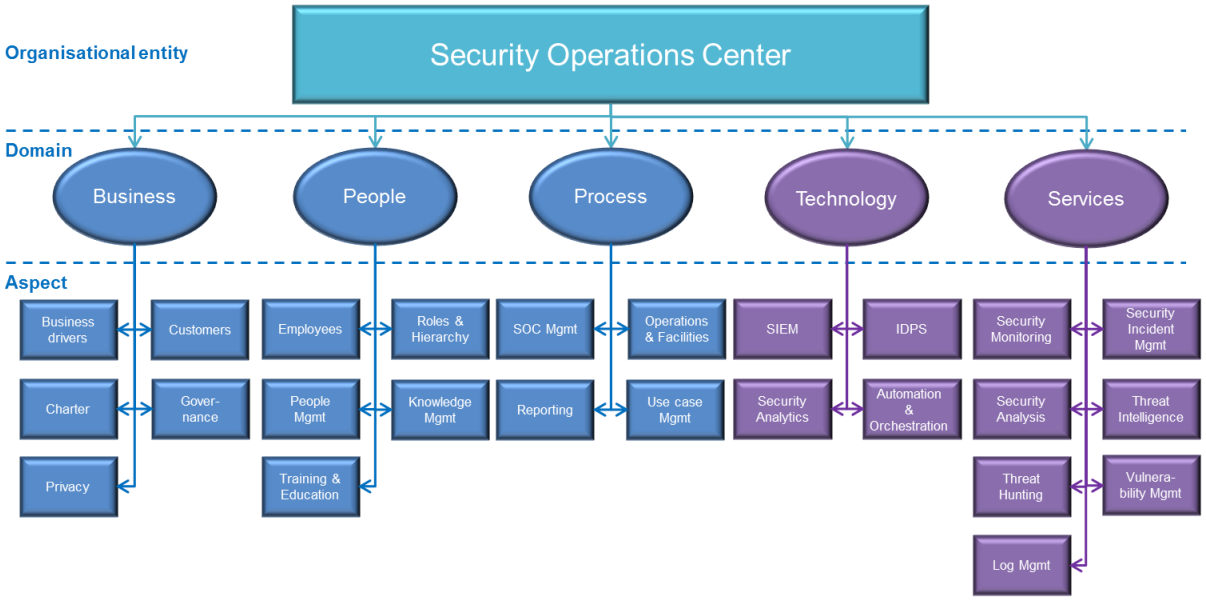
Maturity level	Description
0. Non-existent	At this level, the aspect is extremely ad-hoc or incomplete. Thus, delivery is not assured.
1. Initial	The aspect is delivered in an ad-hoc fashion.
2. Managed	The aspect is documented and delivered consistently.
3. Defined	The aspect is managed using ad-hoc feedback on the quality and timeliness of deliverables.
4. Quantitatively Managed	The aspect is systematically being measured for quality, quantity and timeliness of deliverables.
5. Optimizing	The aspect is continuously being optimized and improved upon.
Capability level	**Description**
0. Incomplete	At this level, the aspect is incomplete. Thus, the SOC has insufficient capability to deliver this aspect.
1. Performed	There is sufficient capability to deliver the aspect at a basic level.
2. Managed	The capability for the aspect is delivered consistently.
3. Defined	The capability for this aspect is optimized and well-documented and delivers true added value.

SOC-CMM Model

SOC modelling is challenging. This is due to the fact that SOCs differ greatly in the set of services they deliver and the technology that they employ. But modelling is required for measurement. The SOC-

CMM was created using a Design Science research approach, in which the gap between theory and practice is bridged by the creation of an artefact. In case of the SOC-CMM, two artefacts have been created: the SOC-CMM model and the self-assessment tool for actual practical measurement.

In order to create the SOC-CMM model, an extensive literature study was conducted. Then, using a survey among 16 participating organizations, all of the elements uncovered in the literature were tested for existence in actual SOCs. The information resulting from the survey was subsequently used to create the SOC-CMM model. This model (in version 1.1) contains 5 domains and 25 aspects or elements and is shown below.



The figure shows the domains 'business', 'people' and 'process' in blue and the domains 'technology' and 'services' in purple. The blue color indicates that only maturity is evaluated. The purple color indicates that both maturity and capability are evaluated.

Usage

While the creation of the SOC-CMM model was an important step in the research, it was not the final step. To create a more concrete result, a self-assessment tool was created and tested in multiple iterations. This self-assessment tool goes beyond modelling and delivers a method of determining the current capability maturity level of any SOC.

There are 2 basic types of assessment: a quick scan and a full assessment. Preferably, the SOC should start out with a full assessment, and then perform a quick-scan to demonstrate progress. A full SOC-CMM assessment is usually carried out by someone outside the team (such as an auditor) or an external assessor. During a full assessment, all aspects of the SOC are investigated, documentation is reviewed, interviews are held and technology and skills are assessed. Quick-scans are normally performed in the form of a workshop. This workshop should be held with several experts within the SOC, preferably with different roles (engineers, analysts, etc.) and different views. By selecting a diverse group of people for the workshop, the workshop is more likely to spark discussion. Such discussion can lead to new insights and provides additional added value besides measurement. Someone outside the team, or even outside the organization, should be used to guide the process,

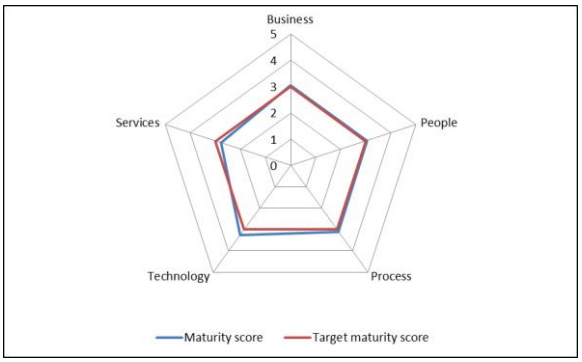
challenge the input provided by participants and thereby increase objectivity and value of the assessment.

The assessment itself is conducted by using the navigation to follow the workflow embedded in the Excel tool. First, a profile and scope is defined. Then, each of the domains is evaluated. This evaluation is performed by choosing the appropriate answer for each of the elements in that domain from a 5-point scale. For each of the maturity questions, guidance will appear once the answer is chosen to aid in selecting the appropriate answer. The scores for each element will result in an aggregated score for the aspect under evaluation and the scores of each aspect will result in an aggregated score for the domain. The difference between the basic and advanced version is that the advanced version supports weighing. That is, determining for each of the elements how important it is to the SOC. While this provides a means for more granular scoring, it can also tamper with the objectivity of the results when used incorrectly. When in doubt, always use the basic version.

Output

Once the assessment has been completed, the results section of the SOC-CMM will show the resulting scores in a table and a graph. A large radar chart shows the score for maturity of each aspect in scope of the assessment. As indicated earlier in this document, capability is only scored on technology and services domains.

2 additional diagrams show the aggregated domain scores for both maturity and capability. If a target maturity level was set in the profile section of the SOC-CMM, the charts will show both the current score and the intended (target) score for the SOC, as displayed in the figures below. The figure on the left shows the aggregated maturity score, while the figure on the right shows the aggregated capability score.



The table provides detailed insight into each domain and helps to determine strengths and weaknesses. Weak aspects in the domain have an adverse effect on the domain as a whole and are candidates for improvement. The improvement plan itself should be created using a risk-based approach. For example, the business domain may not score high, but if there is a more direct risk resulting from the technology domain (even though it scores higher than the business domain), efforts should go into that domain first. Note that insufficient maturity in all domains will eventually pose a risk. Such a risk may not be apparent at first, but may arise later. For example, lack of a sourcing process for new personnel will not affect the SOC while there are sufficient analysts, but may force the SOC into hybrid staffing models or full outsourcing at a later point.

Lastly, the SOC-CMM also provides an alignment to the NIST Cyber Security Framework (CSF). This framework consists of 5 phases: identify, protect, detect, respond and recover. Since the SOC usually has only a limited role in the recovery process, this phase has been omitted from the SOC-CMM. For NIST CSF alignment, each of the individual questions in the assessment was evaluated for relevance to the NIST CSF and mapped to the appropriate element. This mapping is also available on the site as a separate download.

Conclusion

The time in which a Security Operations Center was a buzzword, and every organization wanted one without questioning efficiency or effectiveness, is definitively over. With organizations already running a SOC for a longer period of time, quality becomes more and more important. Capability maturity measurement is a tool that any modern should needs in order to continuously improve and demonstrate added value and return on investment to the business it supports. The SOC-CMM provides a means for self-assessment that allows the SOC to measure its current situation and determine strengths and weaknesses. This information can subsequently be used to plan for- and execute improvement.

So why wait? The SOC-CMM is a free self-assessment tool that can be obtained from the SOC-CMM site. No registration is required. Download the SOC-CMM today and start growing your SOC into a more capable and mature SOC that truly and demonstrably adds value to your organization!

SOC CMM

https://www.soc-cmm.com/

About

The SOC-CMM was created by Rob van Os, MSc. Rob has over a decade of practical experience in security administration, security monitoring, security incident response, security architecture and Security Operations Centers. Rob is currently working as a cyber defense specialist for a SOC in the financial sector and is mainly responsible for day to day security operations and continuous operational improvement.

Rob has obtained a Bachelor's degree in Computer Science from Amsterdam University of Applied Sciences in 2009 and a Master's degree in Information Security from Luleå University of Technology in 2016. Rob also holds several industry certifications, including CEH and CISSP-ISSAP. Rob is also the founder of Argos Cyber Security Assessment, helping organizations growing and maturing their cyber defense teams.