CONTINUOUS IMPROVEMENT ON MATURITY AND CAPABILITY of SECURITY OPERATION CENTERS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF INFORMATICS OF
THE MIDDLE EAST TECHNICAL UNIVERSITY
BY

EFE SUAT ERDUR

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF CYBER SECURITY

DECEMBER 2019

Approval of the thesis:

CONTINUOUS IMPROVEMENT ON MATURITY AND CAPABILITY of SECURITY OPERATION CENTERS

Submitted by Efe Suat Erdur in partial fulfillment of the requirements for the degree of **Master of Science in Cyber Security Department, Middle East Technical University** by,

Prof. Dr. Deniz Zeyrek Bozşahin
Dean, **Graduate School of Informatics** _____

Assoc. Prof. Dr. Aysu Betin Can
Head of Department, **Cyber Security** _____

Assoc. Prof. Dr. Cengiz Acartürk
Supervisor, **Cognitive Science Dept., METU** _____

Examining Committee Members:

Assist. Prof. Dr. Aybar Can Acar
Medical Informatics Dept., METU _____

Assoc. Prof. Dr. Cengiz Acartürk
Cognitive Science Dept., METU _____

Assist. Prof. Dr. Murat Ulubay
Department of Management, Yıldırım Beyazıt University _____

Date: *06.12.2019*

**Write the name of the head of the examining committee in the first row.*
***Write ten name of the supervisor in the second row.*

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: Efe Suat Erdur

Signature : _____

ABSTRACT

CONTINUOUS IMPROVEMENT ON MATURITY AND CAPABILITY of SECURITY OPERATION CENTERS

Erdur, Efe Suat

MSc. Department of Cyber Security

Supervisor: Assoc. Prof. Dr. Cengiz Acartürk

December 2019, 45 pages

This thesis has been studied to define the importance of maturity and capability assessment, and continuous improvement for Security Operation Centers (SOC). Additionally, it aims contribute to the academic literature to fill the research gap in this specific domain as well.

The main focus of this thesis is to combine those two important concepts under same study and define a methodology to provide Security Operation Centers' a self-assessment capability which also evaluates the gaps between current and desired states of the organization and determine the most critical aspects that are suggested to be improved at first.

The applicability of the methodology has been supported with a use case scenario. More importantly, it is evaluated using conversational analysis methodology of qualitative analyze approach and evaluation results have been presented at the final part of the thesis report.

Keywords: Security Operations Center, Maturity and Capability Assessment, Continuous Improvement

ÖZ

SİBER OLAYLARA MÜDAHALE EKİPLERİNİN OLGUNLUK VE YETKİNLİKLERİNİN DEĞERLENDİRİLMESİ VE SÜREKLİ İYİLEŞTİRİLMESİ

Erdur, Efe Suat

Yüksek Lisans, Siber Güvenlik Bölümü

Tez Yöneticisi: Doç. Dr. Cengiz Acartürk

Aralık 2019, 45 sayfa

Bu tez, Siber Olaylara Müdahale Ekipleri'nin (SOME) olgunluk ve yeteneklerinin ölçülmesi ve sürekli iyileştime süreçlerinin önemini vurgulamak ve bu spesifik konuda akademik literatürde bulunan eksikliğin tamamlanmasına yardımcı olmak amacıyla yazılmıştır.

Tezin ana konusu, SOME'lerin gelişimi için önem arz eden bu iki konunun (olgunluk değerlendirmesi ve sürekli iyileştirme) tek bir başlık altında incelenerek bu ekiplere olgunluk ve yetkinliklerinin değerlendirmesini yapabilecekleri, buna ek olarak mevcut ve hedef değerler arasındaki açıklığın değerlendirilmesi yapılarak ekiplere sürekli iyileştirme süreci için gerekli aksiyonların önem derecesine göre sıralı bir biçimde sunulmasını sağlayan bir yöntem sunulmasını amaçlamaktadır.

Önerilen yöntem, örnek bir senaryo üzerinde değerlendirilmiş ve uygulabilirliği gösterilmiştir. Daha önemlisi, önerilen methodoloji konuşma çözümlemesi yöntemi kullanılarak değerlendirilmiş ve sonuçlar tezin son bölümünde açıklanmıştır.

Anahtar Sözcükler: Siber Olaylara Müdahale Ekibi, Olgunluk ve Yetkinlik Değerlendirmesi, Srekli İyileştirme

To My Family

ACKNOWLEDGMENTS

First of all, I would like to express my sincere gratitude to my advisor Assoc. Prof. Dr. Cengiz Acartürk for the continuous support throughout my thesis study for his patience and absolute motivation. His door was always open for me whenever I ran into a trouble or I had a question about my research. This accomplishment would not have been possible without him.

Besides my advisor, I would like to thank to my thesis jury members, Assist. Prof. Dr. Aybar Can Acar and Assist. Prof. Dr. Murat Ulubay for their suggestions and reviewing my work.

I would also wish to express my gratitude to the experts who have shared their precious time during the process of interviewing. Without their passionate participation, the evaluation of this study could not have been successfully conducted.

I would also like to give special thanks to Murat Çakır for being a mentor to me throughout this study and for his continuous encouragement for any kind of new challenges in my career, and Erdem Kivci for providing me extensive personal and professional guidance.

Above all, I wish to thank to my wife, Damla Erdur, for her love and constant support during not only this study but also for life.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CA	Conversation Analysis
CI	Continuous Improvement
CMM	Capability Maturity Model
CMMI	CMM Integration
COBIT	Control Objectives for Information and related Technology
CTQ	Critical to Quality
DMAIC	Define, Measure, Analyze, Improve, Control
IT-IS	Information Security Incident Management
IR	Incident Response
MDR	Managed Detection and Response
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PDCA	Plan-Do-Check-Act
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center

CHAPTER 1

INTRODUCTION

Rapid developments in information and communication technology are changing individual lifestyles and business conduct, and this situation creates wide range of new business domains. Concordantly; tactics, techniques and procedures of adverse such as hacking, viruses and personal information leaking are also rapidly improving (Park, Jang, & Park, 2010). In order to be successful against rapidly improving adversaries, cyber security teams have to be improving themselves and adapting to new updates as well. However, the frequent changes in an organization require a systematic alignment of business processes on business strategies (Nassar, Badr, Biennier, & Barbar, 2012). This thesis aims to investigate adaptation of Security Operation Center (SOC) organizations to such rapid changes and to investigate possible methodologies to apply to SOCs in terms of systematic improvement.

The responsibility of SOC can be defined as monitoring, detecting, investigating and isolating incidents in the network and the management of the organization's security products, network devices, end-user devices, and systems (McAfee Foundstone, 2016). The new generation of SOCs are enriching their processes by including advanced technologies such as threat intelligence, threat hunting and/or cognitive security. However, there is a gap in the architectural management and continuous improvement of such organizations because there is limited formal research and awareness on this domain (Van Os, 2016).

According to Hewlett Packard Enterprise examination which held on 2017 over 140 SOCs in more than 180 assessments around the globe, the majority of cyber defense organization's maturity remains below target levels. Their investigation declares that "82 percent of SOCs are failing to meet their criteria and falling below the optimal maturity level and 27% of the SOCs are failing to achieve minimum security monitoring capabilities." (Hewlett Packard Enterprise , January, 2017). This situation results in many vulnerabilities in the event of an attack and it is obvious that all security operation teams should be focusing on continuous improvement of their operations.

According to the Jugdev and Thomas; maturity models identify project or organizational strengths, weaknesses and benchmarking information (Judgev & Thomas, 2002). Maturity and capability assessment models are useful for any kind of organizations to self-assess their current maturity and capabilities, and also analyze the

results to understand ‘what to improve’. However, such models cannot answer the question; ‘how to improve’. In this study, continuous improvement (CI) and maturity and capability assessment are combined in order to propose a methodology to fill the gap on lack of understanding of maturity and capability of SOC teams and improve their process quality by proper continuous improvement procedures.

1.1. Problem Definition and Motivation

There is limited formal research on measurement of maturity and capability of SOCs. Van Os, in his thesis work, has investigated common maturity integration models, suggested his own framework and created a self-assessment tool for SOC teams to assess their maturity levels (Van Os, 2016). His study provides satisfying results for self-assessment; however, the improvement methods of the organization is not covered in his work.

Also, cyber security companies that are providing security operation or consulting services to their customers have been partly sharing their frameworks with public. For example, Aujas, the IT security company, provides a measurement framework to measure maturity of information security incident management (Suryawanshi, 2018). Another cyber security company, CREST, provides a similar assessment tool for incident response service (CREST , 2018). Although both of the frameworks are based on incident management service rather than whole SOC organization, the model they are presenting serves as a model for any kind of assessment domain.

All the mentioned frameworks offer beneficial methodologies to assess maturity and capability, however they stand at the assessment part and do not include systematic improvement methodology. This gap prevents the teams to improve themselves in a systematic procedure which causes significant vulnerabilities on security services and inadequacy on the quality of service outputs.

1.2. Research Question

Briefly summarizing the problem which is explained above, the research question can be defined as;

How can the maturity and capability levels of security operation centers be assessed properly and required improvement steps could be determined and implemented in order to increase the maturity of the organization to expected levels?

1.3. Hypothesis

Considering the defined problem above, the hypothesis can be defined as;

A methodology could be created for SOCs to continuously improve their organizations in the lights of maturity and capability assessment results so that they can increase their maturity and capability to expected levels.

1.4. Scope

Although continuous improvement is a crucial concept for all organizations, the scope of this thesis has focused on SOC teams.

Also, in this paper, the research is limited with technical aspects of the problem, so no business level investigations are included in the scope.

Finally, although there are many services could be defined under a SOC, the scope is limited only with 'Incident Handling/Response' service. Investigating other possible services or aspects are defined as the future work.

1.5. Thesis Outline

This thesis report consists 5 chapters;

1. Introduction: Current chapter includes an introduction to the thesis study, problem definition and overview of work done in this thesis study.

2. Relevant Work and Literature Review: This chapter includes all the literature review results of investigation which are used to support the hypothesis.

3. Design and Methodology: In this chapter, the work of this study is presented, and the hypothesis is tried to be strengthened by providing all supportive work.

4. Results: Results of the work are presented in this chapter, and possible future works are suggested succeeding the results.

5. Conclusion: A final discussion about the methodology and conclusion part of the thesis report are included in this final chapter.

CHAPTER 2

RELEVANT WORK AND LITERATURE REVIEW

The focus of this study is to create a continuous improvement methodology for a specific organization, SOC. Therefore, the literature research starts with investigating current continuous improvement (CI) frameworks/methodologies and tools that are used in such frameworks. Comparing those frameworks in terms of their usage areas and evaluation of their advantages and disadvantages are also studied in this part in order to understand which framework would be the best fit for the purpose of this study.

Second step of literature research is investigating current capability and maturity models for SOC organizations. Studying on such a model is crucial because assessment of the organization is one of the core parts of continuous improvement process.

For the CI methodology that is studied in this thesis, there are many SOC services that could be worked on, as it is illustrated in current capability and maturity models investigation. The number of services that any SOC organization is offering to their customers could be high and working on each of them is a tough individual task. For this reason, the scope of this study is limited to work on only "Incident Handling/Response" service. Therefore, in the final part of this chapter, the possible methods to improve "Incident Handling/Response" service have been investigated and results are presented.

2.1. Continuous Improvement Models

One of the oldest but a popular definition of CI is: "a broad change program, planned, organized and systematic, and distinguished from project-based models of change" (Lindberg & Berger, 1997). American Society for Quality defines CI as the ongoing improvement of products, services or processes through incremental and breakthrough improvements (American Society for Quality, n.d.). These definitions show that CI is an improvement process, and it can be applied to products, services or processes. In this thesis study, applying CI over services and processes rather than products has been

focused. The first challenge at this point was to determine which CI approach fits best for the purpose of this study. For this reason, first step of the literature research was investigating common continuous improvement methodologies and determine which methodology or combination of multiple methodologies have best fit with the hypothesis.

There exist many CI approaches in the literature and many investigation papers has been created over each of them. For example; de Mast and Lokkerbol has investigated Six Sigma DMAIC method from problem solving perspective. They have selected five problem solving methodologies from literature and studied investigating them from DMAIC perspective (de Mast & Lokkerbol, 2012). The aim at this point was to compare such approaches and Sokovic, Pavletic and Pipan have already studied about the comparison of PDCA, Radar Matrix, DMAIC, DFSS in their work (Sokovic, Pavletic, & Pipan, 2010). Following figure shows comparison of the steps of those methodologies.

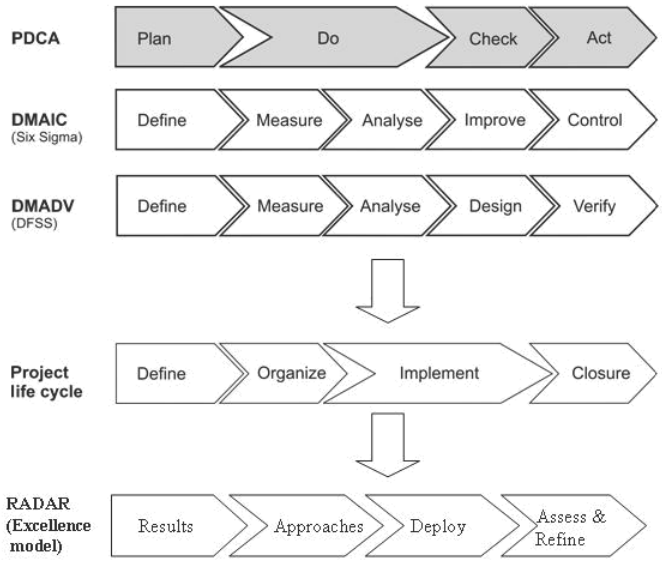

Figure 1: The PDCA cycle vs. DMAIC (Six Sigma), DMADV (DFSS), the Project-Life Cycle (PLC) and RADAR (Excellence model), (Sokovic, Pavletic, & Pipan, 2010)

Their work does not only cover the processual comparison among those improvement methodologies but also the possible usage domains of each methodology in terms of product, process and services in organizations.

According to finding of their study, PDCA cycle is a simple but effective methodology for CI process which could be used by large number of people in the organization. Another benefit is after 'act' stage is completed, the cycle could start again for forthcoming improvements. (Sokovic, Pavletic, & Pipan, 2010) Considering the disadvantages of PDCA, it would not be the best way of SOC organization; however,

the simplicity and adaptation to rapid changes functionalities are making it a proper methodology to apply for service level continuous improvements within big picture.

DFSS is a disciplined methodology including all required functionalities from the beginning, therefore this approach is suggested as a best fit for new products or processes (Sokovic, Pavletic, & Pipan, 2010). The scope of this study is SOC organizations which are already active and giving service to their customers or own organizations, and interruptions or re-constructions in the service are out of question unless there are crucial problems in the core architecture of the current service. Therefore, DFSS does not seem to be the best fit for the purpose.

RADAR methodology is also defined as a strategic, systematic, fact-based framework which is based on EFQM excellence model. Similar with DFSS, RADAR also determined as complex and powerful methodology which is longer-term and resource demanding process (Sokovic, Pavletic, & Pipan, 2010). Such excellence models are offered as a best fit for project planning and improvements, but not such a best fit for active, dynamic and rapidly changing services like SOC services.

DMAIC methodology of Six Sigma approach, on the other hand, has been defined as systematic, fact based, and data driven methodology which could be a proper option for flexible processes. Hence it is defined as a data driven approach, assessment is the crucial part of DMAIC in the define (D) phase. The process cannot be measured unless it is defined properly, therefore it is not possible to utilize DMAIC in improvement actions (Sokovic, Pavletic, & Pipan, 2010). This requirement of the methodology has a perfect match with the thesis problem, because maturity and capability assessment of current organization is the key point to improve any SOC organization as it was stated earlier.

Figure-2 shows the flows of DMAIC cycle. Another characteristic of DMIAC is, it can be used to create gated processes, in a cycle. SOC organization has multiple ‘services’ which can be accepted as individual projects of organization, therefore this characteristic of DMAIC will be also useful for CI for SOC.

2.2. Maturity Assessment on SOC

DMAIC highly depends on statistical measurements as it was stated earlier and next step for the literature research was investigating measurement methodologies for SOC organizations.

In order to assess an organization, capability and maturity assessment models are used. A capability maturity model is defined as a tool that helps people to assess the current effectiveness of a person or group and supports figuring out what capabilities they need to acquire next in order to improve their performance (De Bruin, Tonia, Freeze, Ronald, Kaulkarni, Uday, & Rosemann, Michael , 2005). Derivatively, a cybersecurity maturity model is a framework for measuring the maturity of a security program and guidance on what to do to reach the next level.

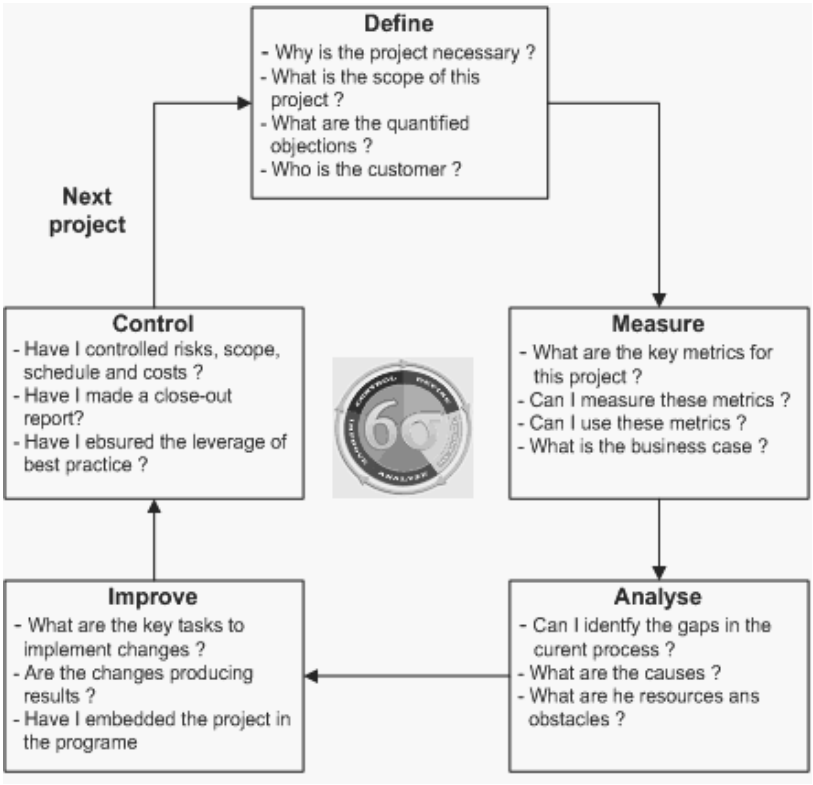

Figure 2: The DMAIC cycle as a methodology of Six Sigma (Sokovic, Pavletic, & Pipan, 2010)

Although there exist capability and maturity models which are defined for cyber security, information security and IT domains, currently there is no maturity model or common framework available specific to security operation teams which is defined by authorities. OWASP has an open project for such purpose, and in the definition of the project they state that there is no such framework available from any government, non-government or commercial organization currently. (OWASP Security Operations Center (SOC) Framework Project, 2019). Performing a literature research to deciding on a such a model for assessment purpose is the main goal of this part of the literature research.

2.2.1. Maturity and Capability Models for Cyber Security Domain

2.2.1.1. SOC-CMM Model

Rob van Os, in his study, used a top-down approach where the maturity levels are defined first and the characteristics are filled in later (Van Os, 2016). In his work, he defined the maturity levels starting at level 0 (non-existent) up to level 5 (optimizing), and as the naming convention he used the names which are defined in CMMI (CMMI Institute, 2017).

The maturity levels that are defined in his work are;
- Level 0: non-existent,
- Level 1: initial
- Level 2: managed
- Level 3: defined
- Level 4: quantitatively managed
- Level 5: optimizing

And the capability levels that is defined in his work are;
- Level 0: incomplete
- Level 1: performed
- Level 2: managed
- Level 3: defined

In this work, van Os also investigated all other limited resources in detail, followed a proactive research methodology and proposed a continuous representation for capability and maturity levels for SOC teams. Moreover, he defined an organizational model for SOC including 23 aspects for 5 domains (business, people, process, technology and services), and he created a tool to measure maturity and capability levels of any SOC organization.

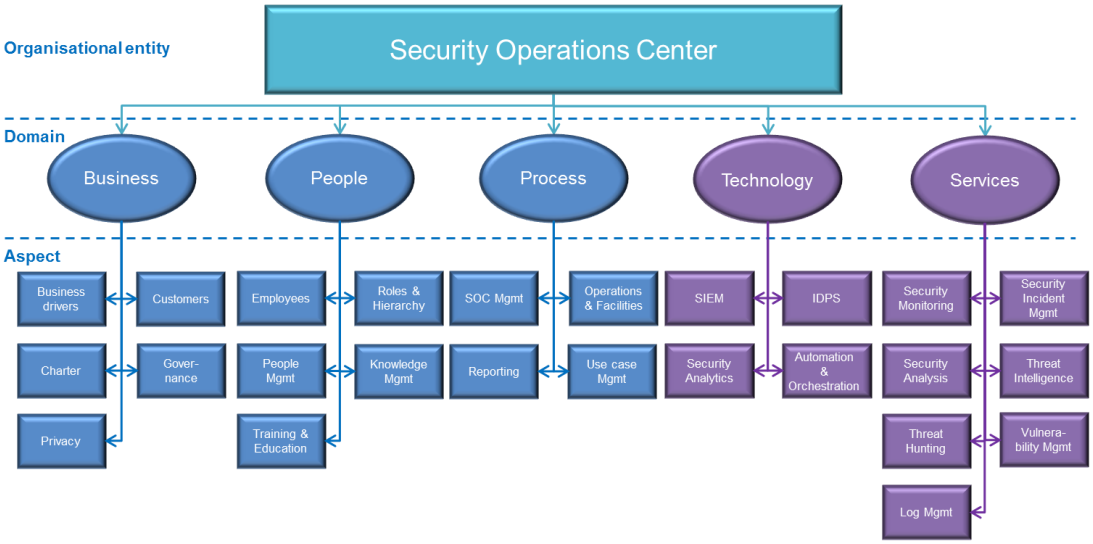

Figure 3: SOC Capability Maturity Assessment Model (Van Os, 2016)

The result of the assessment tool was a radar chart which visualizes maturity and capability levels of all the domains and aspects that are defined in the organizational model.

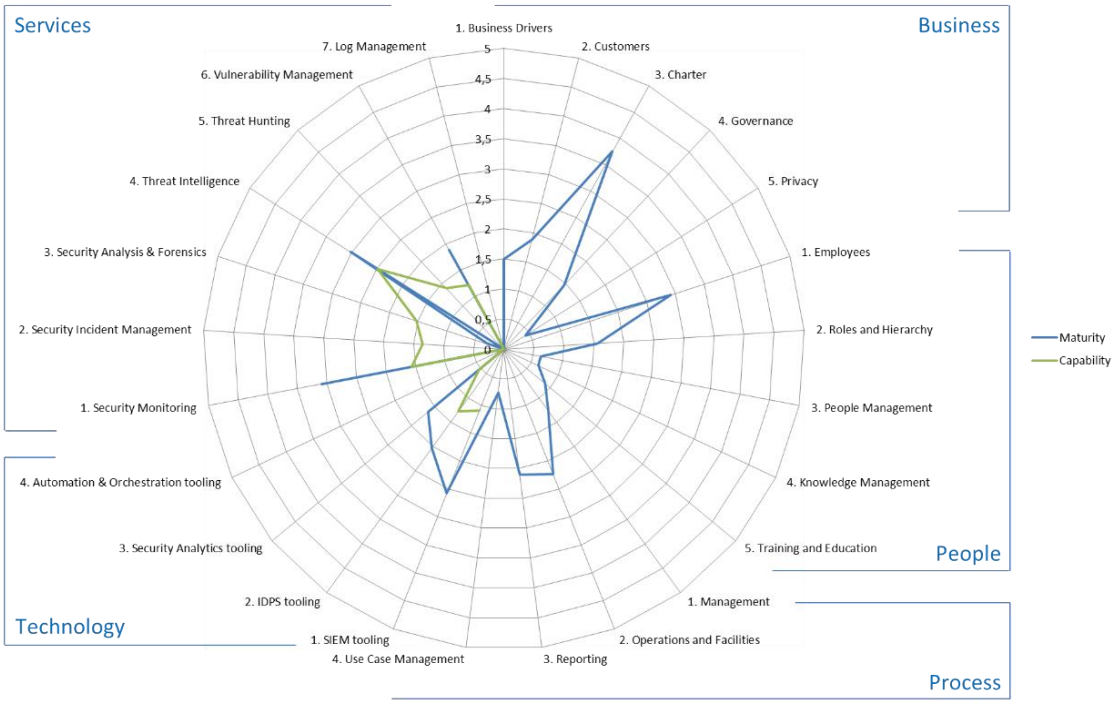

Figure 4: Maturity and Capability Scores Visualization (Van Os, 2016)

2.2.1.2.Classification of Security Operation Centers

Jacobs, Arnab and Irwin have made a useful research about classification for security operations centers (Jacobs, Arnab, & Irwin, 2013). In their study, they researched industry accepted maturity levels for cybersecurity and IT domain including Control Objectives for Information Technology (CoBIT), Information Technology Information Library (ITIL), and also security frameworks such as ISO/IEC 27001. As a result of their work, they created a comparison table among those models and published their model under six levels such as;

Table 1: Process Maturity (Jacobs, Arnab, & Irwin, 2013)

Level	Name	Alignment
0	Non-Existent	CoBIT 0, etc.
1	Initial	CoBIT, SSE, ITIL: Initial CERT: Exists
2	Repeatable	(CoBIT, ITIL, SSE-CMM and CERT/CSO)
3	Defined Process	(CERT/CSO) / Well Defined (SSE-CMM), Defined Process (CoBIT), Common Practice (CITI-ISEM)
4	Reviewed and updated	(CERT/CSO), Quantitatively controlled (SSE-CMM), Managed and Measurable (CoBIT) and Continuous Improvement (CITI-ISEM)
5	Continuously Optimized	Optimized (CoBIT), Continuously Improving (CITI-ISEM), Continuously Improving (SSE-CMM)

2.2.1.3. CMMI

CMMI (Capability Maturity Model Integration) has developed by Software Engineering Institute of Carnegie Mellon University which defines CMMI as a capability improvement model that can be adapted to solve any performance issue at any level of the organization in any industry (CMMI Institute, 2017). It breaks down organizational maturity into five levels which are labelled as;

Maturity Level 1 Initial
Maturity Level 2 Managed
Maturity Level 3 Defined
Maturity Level 4 Quantitatively Managed
Maturity Level 5 Optimizing

2.3. Incident Handling Assessment

According to survey which is done by Van Os among 16 participants of SOC organizations, the most critical three processes among others were determined as "*Security Incident Management*", "*Security Monitoring*" and "*Security Analysis*" (Van Os, 2016). These processes can be defined as the components more generic service "Incident Handling/Response". For this reason, the scope of this study is limited with "Incident Handling/Response Service". However, the same methodology can be applied to each of the other services as well.

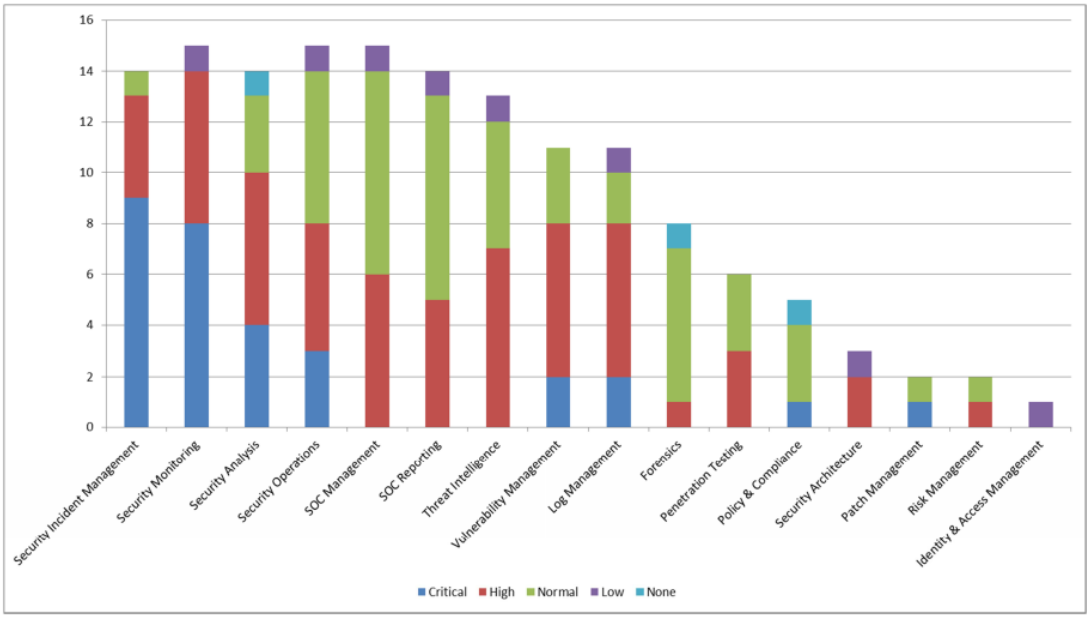

Figure 5: SOC process activities - criticality of services (Van Os, 2016)

At this point, it should be emphasized again that improving one specific service is only one component of the big picture. After a SOC is analyzed, maturity and capability assessment is completed, and it is determined that incident handling service needs improvement; the following process is also internal CI process that should be measured, analyzed and improved individually. For this reason, the assessment and improvement methodologies of incident handling/response were also investigated in this chapter.

This chapter -*2.3*- is allocated for the literature research of such framework. Unfortunately, the academic literature gap that was mentioned previously is valid for service-based maturity assessments as well. Moreover, the processes of the services are relative to the organization and although there are some common processes on all security companies, most processes of services could differ from each other. For this reason, it was not very likely to find academic records for such generic definitions and this part of literature research is focused more on cyber security companies' open source frameworks.

2.3.1. Aujas IS-IM Framework Maturity Measurement

AUJAS is a global IT risk management (IRM) company that offers a demonstration version of Information Security and Incident Management (IS-IM) framework –an excel tool- for maturity management. Their maturity model is built in line with CoBIT, ISO 27035 and NIST 800-83 standard as a base for guidance (Suryawanshi, 2018).

In this framework, the maturity of IS-IM is measured across five domains - Governance, People, Process and Technology for Monitoring, Prevention against malicious Code and Networking. For each domain, the tool asks user to fill a questionnaire using a number from 1 to 5 for estimated maturity level for the capability which belongs to that domain. Following figure is an example for very small part of the whole questionnaire.

DOMAIN RATING		0,92		1,62	
Aujas Networks - Information Security Incident Management's Maturity Assessment					
Information Gathering - Process - Information Security Incident Management's					
S. No.	Tool		Maturity	Observation Before IS-IM Program	Maturity	Response post IS-IM Program
	Management Commitment / Approval, Monitoring and Reporting	Source	0 to 5		0 to 5	
1,01	There exists an documented and approved information security incident management policy and processes with defined purpose and clear objectives, roles and responsibilities and reporting	NIST 80-061		An IS-IM procedure existed with clear objectives but not with detailed roles and responsibilities and mechanism to report and track information security incidents		A detailed roles and responsibilities with clear interaction model is defined
1,02	The IS-IM policy, Process and procedure documents are approved by the Management	ISO27001		VP-CA approved the process and procedure for IS-IM		VP-CA approved the process and procedure for IS-IM
1,03	The IS-IM policy and process documents are communicated with all the stakeholders and awareness conducted to various stakeholders for handling information security incident	NIST 80-061		The IS-IM had certain groups like ISIRT charter, members identified but no training and awareness provided to the required stakeholders.		Training is provided to ISIRT members and R&R awareness created
1,04	An ISIRT charter is defined to address scope, limitations, communication and interaction, authority and responsibility to manage information security incidents	ISO 27001		ISIRT charter does not exist		ISIRT charter created
1,05	Incident reporting mechanism is established for reporting of information security events and Communication plan is established to contact specific individual during incident	NIST 80-061		There is no specific mechanism established to report information security incident, it is primarily via emails to ISO / CISO		Reporting mechanism defined to Helpdesk / email and contact but automation of incident and tracking should be done as a part of further phase

Figure 6: Example image of process assessment from IS-IM Framework (Suryawanshi, 2018)

After the user provides all estimated maturity levels, the tool shows the maturity score under the score sheet as shown in the following image.

Domains	
1. IS-IM Governance (Policy / Procedure/ Reporting / R&R, Metrics and Audit)	0,92
2. IS-IM Process (Process / Procedure/ Templates)	1,51
3. People (Training, Awareness, JDs/Staffing / Response arrangement)	2,13
4. Technology - Monitoring (IS-IM technology controls for detection and response/ reporting and measurement)	2,24
4. Technology - Malicious Code (IS-IM technology controls for detection and response/ reporting and measurement)	2,70
4. Technology - Network (IS-IM technology controls for detection and response/ reporting and measurement)	2,97

Figure 7: Maturity results of assessment from IS-IM Framework (Suryawanshi, 2018)

2.3.2. CREST - Cyber Security Incident Response Maturity Assessment

CREST is a non-for-profit organization which focuses on creating technical knowledge to security world (CREST , 2018). Similar to Aujas, they are providing a measurement assessment tool for cyber security incident response. This tool collects data from user among three phases; Prepare, Respond and Follow-Up. The user inputs its data as configuration (target state) and assessment (current state), then the maturity scores are presented in a radar chart to user. Hence it asks for target and current state, the gap between those states are also could be checked from the radar chart which is shown in image below.

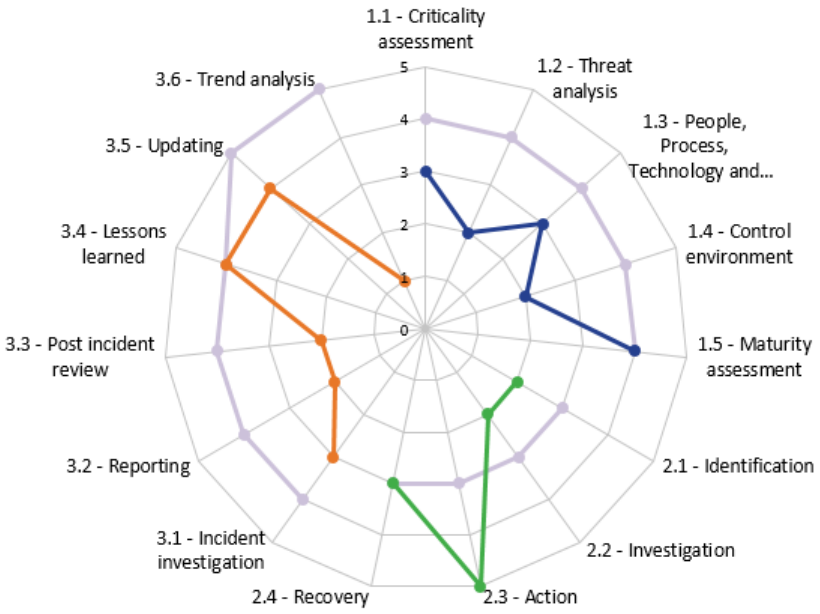

Figure 8: Assessment results of CREST framework (CREST , 2018)

2.4. Incident Handling/Response Service Improvement

In this section of the literature research, improvement methods of 'Incident Handling/Response' service of SOC organization is studied. The research done here provided a good vision about experts' reviews on improving this specific service and the results are highly used when defining the methodology.

Handling incidents in cyber security teams is an interesting and popular concept among cyber security world and the technical literature about this topic is rich. However, this study focuses on improving how this service is offered rather than how to handle a single incident. This topic highly depends on internal resources of the organization such as goals of the organization, customer expectations, business requirements and any many other similar parameters. Therefore, there were challenges in finding academic resources and the research point was redirected to the cyber security experts' reviews on blogs or web pages and their suggestions about this specific subject.

One of the suggestions for improving incident response (IR) service that Wichman describes in his work is automation (Wichman, 2018). He describes that automation of repetitive manual tasks is a critical improvement for this service and it makes team to detect, analyze and respond high risk incidents quicker. He also refers to Optiv research which claims that average time of handling and incident decreases about %96 with proper automations.

Another improvement that Wichman suggests is orchestration which enables the organization to use their human resources properly in the automation part of the process (Wichman, 2018). Therefore, it can be concluded that orchestration aligns all people, process and technologies to satisfy service requirements.

A cyber security company, CyberSponse, also offers some improvement about this topic. Among many suggestions that they are offering, the importance of collecting metrics must be emphasized to improve detection parameters and improvement of the service (CyberSponse, 2018). In addition to that, they also describe the importance of orchestration and the company is actively developing an orchestration tool improve service quality.

Dan Holloran also indicates the importance of defining and using metrics in his work to improve incident response service (Holloran, 2018). He explains that such improvement will helps the team to avoid alert fatigue start responding to incidents that actually matter.

As the result of investigation about this part, following table was created to state the dependency of incident handling/response service over other domains in SOC maturity model.

Table 2: Idea and required actions for improving incident handling service

Improvement Idea	**Reference**	**Required Action to Accomplish**
Automate	(Wichman, 2018)	1. Define automation **process** 2. Use automation **technology**
Orchestrate	(Wichman, 2018) (CyberSponse, 2018)	1. Include human –**people**- control in the automation **process**. 2. Improve you incident handling/response tools – **technology**- to include orhestration.
Focus on Relevant Metrics Measuring Success	(CyberSponse, 2018) (Holloran, 2018)	3. Include metrics to **processes** to evaluate and improve performance of team - **people**.

This investigation shows that improving a service -*Incident Handling/Response Service in this case*- directly depends on people, process and technology triangle. As a result, although the organizational model that is suggested by van Os in figure 3 is a useful chart for maturity and capability assessment, it is not likely to apply an iterative CI methodology to services defined in the model. Therefore, following updated model is suggested for CI over SOC organizations.

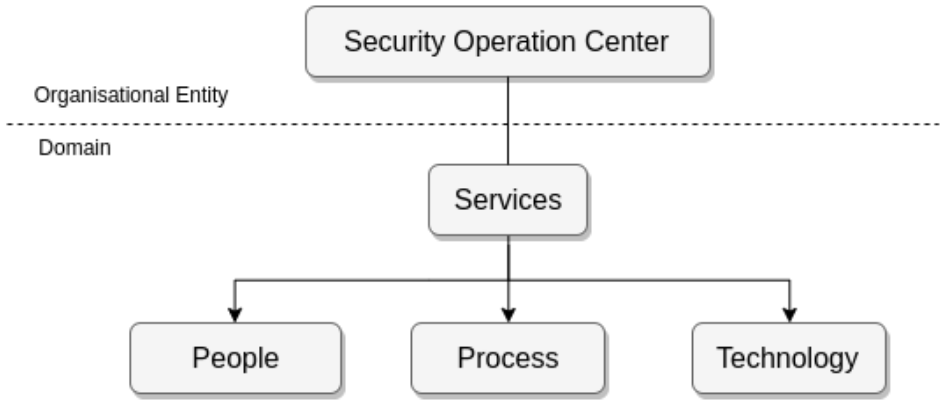

Figure 9: Updated SOC Assessment Model

Also, the 'Business' domain is removed from organizational chart hence it is mostly related to enterprise side of the operations whereas the focus of this study covers the technical side of the problem.

CHAPTER 3

DESIGN AND METHODOLOGY

3.1. Overview

Six Sigma -*and many other CI approaches*- focuses on 'how' to improve a service or a product, but they cannot provide what to improve. On the other hand, the capability and maturity models for SOC organizations that was introduced in the literature research provide the visibility of 'what' to improve in terms of reporting current maturity levels of organizational services and calculating the gap between current and desired states of each service of the organization.

The focus in this methodology was to combine those approaches and to provide a full scope of continuous improvement methodology for SOC organizations. DMAIC methodology of Six Sigma approach was used in organizational level in order to satisfy this requirement. Additionally, improvement of each service in the whole organization was a specific job which must be evaluated and processed separately. For such purpose, PDCA cycle was applied in service level improvements because of the simplicity and adaptation to rapid changes of the approach.

In short, the methodology that defined in this chapter aims to propose a guideline in order to apply continuous improvement on security operation center processes using Six Sigma DMAIC methodology and PDCA cycle combined. The models, methodologies or tools that were used as reference to create the proposed methodology are summarized in the table below.

Table 3: Resource Table

Function	**Resource**
CI on Organizational Level	Six Sigma (DMIAC) Methodology
CI on Service Level	PDCA Methodology
SOC Capability and Maturity Assessment	Updated version of Van Os' CMM
"Incident Handling/Response" Assessment	CMM of IS-IM Framework of Aujas

Following figure illustrates the overview of the planned CI methodology on SOC.

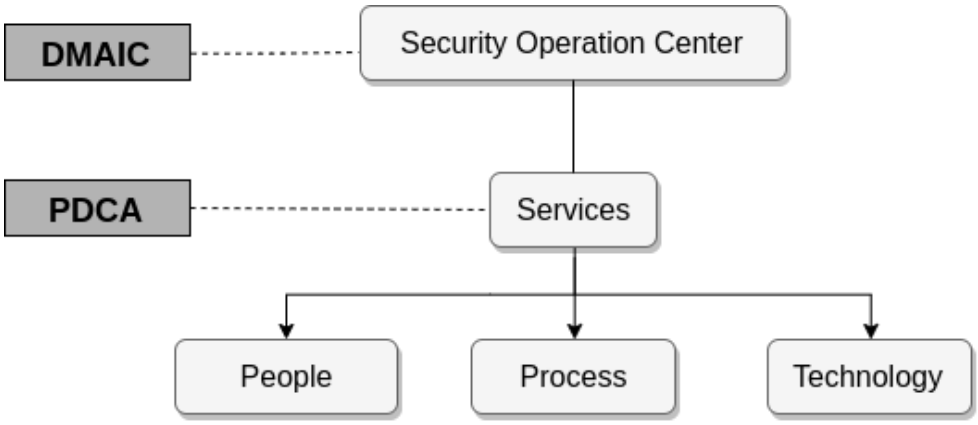

Figure 10: CI over SOC methodology in organizational level and service level

3.2. Six Sigma in the Service Industry

Although *Six Sigma* was created for manufacturing companies at first, it rapidly expanded to different areas such as marketing, engineering, purchasing, servicing, and administrative support, as the organizations noticed the benefits of the approach (Kwaka & Anbari, 2004). In the service-oriented domain, it has been used in industries such as financial services, healthcare industry, telecommunication services, utility companies and airline industry. (Antony, 2006)

Figure-11 shows the potential applications of six sigma within service processes. (Antony, 2006)

As a more specific example, Aazadnia and Fasanghari have applied Six Sigma to information technology service management (ITSM) in terms of CI (Aazadnia & Fasanghari, 2008). In their work, they combined Information Technology Infrastructure Library (ITIL) -*which includes set of guidelines that specify what an IT organization should do*- and DMAIC methodology of Six Sigma in order to provide a better methodology for improving the quality of IT service.

Type of service function	Potential areas where six sigma may be employed
Banking	Wire transfer processing time, number of processing errors, number of customer complaints received per month, number of ATM breakdowns, duration of ATM breakdowns, etc.
Healthcare	Proportion of medical errors, time to be admitted in an emergency room, number of successful surgical operations per week, number of wrong diagnoses, waiting time to be served at the reception in a hospital, etc.
Accounting and finance	Payment errors, invoicing errors, errors in inventory, inaccurate report of income, inaccurate report of cash flow, etc.
Public utilities	Late delivery of service, number of billing errors, waiting time to restore the service after a fault has been reported, call centre of the utility company, etc.
Shipping and transportation	Wrong shipment of items, wrong shipment address, late shipment, wrong customer order, etc.
Airline industry	Baggage handling, number of mistakes in reservation, waiting time at the check-in counter, etc.

Figure 11: Potential applications of six sigma within service processes. (Antony, 2006)

3.3. Applying Six Sigma DMAIC to SOC Improvement

DMAIC methodology of Six Sigma approach has well-defined 5 steps which are problem definition (D), measurement of the problem (M), data analysis (D), improvement process (I) and controlling (C) or monitoring process to prevent recurring problems. (Aazadnia & Fasanghari, 2008) Following figure shows the flow of the methodology.

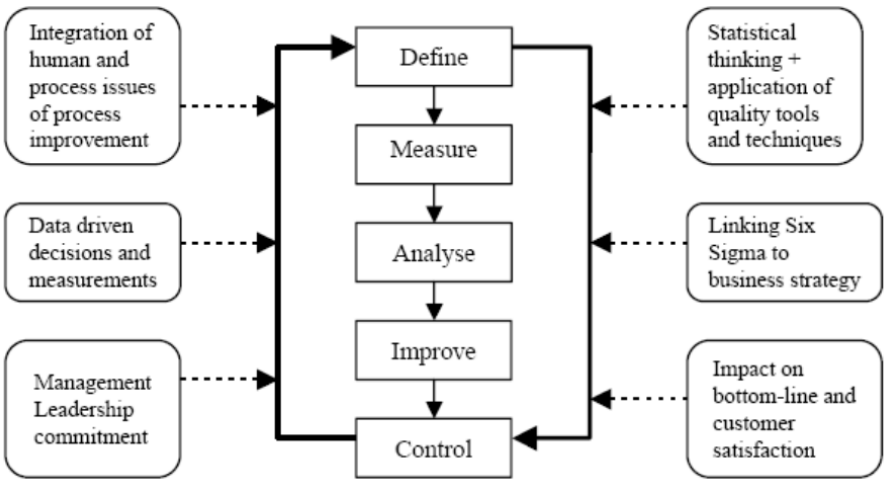

Figure 12: Six Sigma methodology (Aazadnia & Fasanghari, 2008)

In this study, each phase of DMAIC was applied for SOC organization considering the characteristic functionalities of the specific security service. DMAIC is an iterative process and the deliverables of each phase would provide input the next phase. Therefore, the suggested deliverable list for each phase of the process is defined, which are gathered from literature and optimized for the benefit of SOC organizations.

Additionally, De Koning and De Mast also worked on reconstructing DMAIC processes in problem solving approach and they created following table as reference to show rational reconstruction of each phase of the methodology (De Koning & De Mast, 2006).

Table 1
Rational reconstruction of the DMAIC procedure, after De Koning and De Mast (2006).

Define: problem selection and benefit analysis
D1. Identify and map relevant processes
D2. Identify stakeholders
D3. Determine and prioritize customer needs and requirements
D4. Make a business case for the project

Measure: translation of the problem into a measurable form, and measurement of the current situation; refined definition of objectives
M1. Select one or more CTQs
M2. Determine operational definitions for CTQs and requirements
M3. Validate measurement systems of the CTQs
M4. Assess the current process capability
M5. Define objectives

Analyze: identification of influence factors and causes that determine the CTQs' behavior
A1. Identify potential influence factors
A2. Select the vital few influence factors

Improve: design and implementation of adjustments to the process to improve the performance of the CTQs
I1. Quantify relationships between Xs and CTQs
I2. Design actions to modify the process or settings of influence factors in such a way that the CTQs are optimized
I3. Conduct pilot test of improvement actions

Control: empirical verification of the project's results and adjustment of the process management and control system in order that improvements are sustainable
C1. Determine the new process capability
C2. Implement control plans

Figure 13: Rational Reconstruction of the DMAIC Procedure (De Koning & De Mast, 2006)

3.3.1. Phase 1 – Define

In this phase, the first step is defining scope and objectives of the organization.

For a SOC team, the scope definition starts with determining which services are expected to be provided. The number and type of services that are provided by a SOC organization could vary. For example, van Os has defined seven services for SOC in his model which are "*Security Monitoring, Security Incident Management, Security Analysis & Forensics, Threat intelligence, Threat Hunting, Vulnerability Management*

and Log Management" (Van Os, 2016). MITRE, on the other hand, has defined the services of a SOC listed as; "*Real-Time Analysis, Intel and Trending, Incident Analysis and Response, Artifact Analysis, SOC Tool Life-Cycle Support, Audit and Insider Threat, Scanning and Assessment, Outreach*" (Zimmerman, 2014).

Although the service types could vary in different sources, some of the services are called with different naming conventions although they are practically same or very similar. For example;

"Security Monitoring" (Van Os) maps to "Real Time Analysis" (MITRE)

"Threat Intelligence" (Van Os) maps to "Intel and Trending" (MITRE)

"Security Incident Mng." (Van Os) maps to "Incident Analysis & Response" (MITRE)

"SOC Tool Life-Cycle Support" (MITRE) has no exact mapping on Van Os' work.

In any case, the services that are provided or expected to be provided by the current organization should be determined and defined in order to clarify the scope of the organization as the first job.

Next step is identifying the stakeholders. Any people or organization that are affected by SOC could be defined as stakeholder; however, they could be prioritized regarding the authority they have over the project and their interests to project. Following matrix has defined for prioritization of stakeholders (Júnior, Porto, Pacifico, & Júnior, 2015).

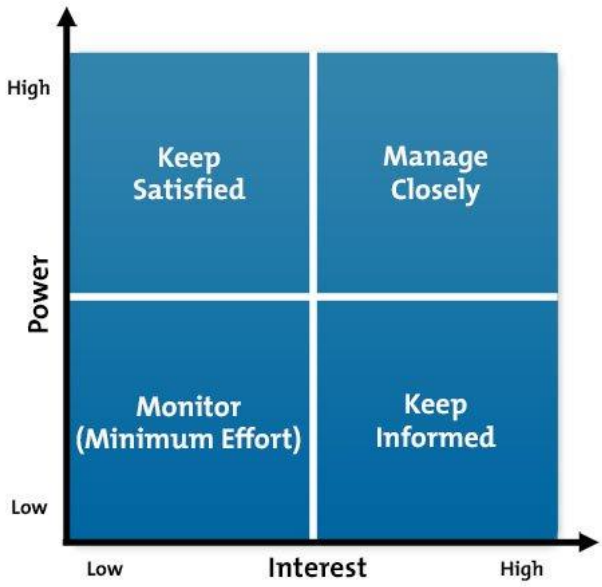

Figure 14: Power / Interest Matrix (Júnior, Porto, Pacifico, & Júnior, 2015)

Regarding this model, the people with high power and high interest engaged as stakeholders directly and roadmap of projects should be determined together.

Other people in the stakeholder list could be determined as lower priority, and they should be satisfied, informed or allowed to monitor the updates in the project regarding their positions on the power-interest grid.

A SOC team can be in-house or external. An in-house SOC is a team who belongs to the company whereas an external SOC is an outsourced service. The difference between these two organization types does not affect processes, services or outputs of the SOC significantly; however, it affects scope of the project, stakeholder definitions and budget of the project directly. In an in-house SOC, the stakeholders could be senior executives, cyber security experts or analysts; on the other hand, in an outsourced SOC, customer has to be included in the stakeholders as well.

Stakeholders' expectations and metrics together are called as Critical to Quality (CTQ) definitions (Singh & Khanduja, 2012). In other words, CTQ includes which services or processes are critical to SOC team, and what are the target requirements of the organization. For this reason, defining stakeholders correctly is the key stage of CTQ definitions.

The deliveries should be created at this phase are;

1. Scope and goals
2. Stakeholder analysis
3. Budget planning
4. Critical to Quality (CTQ) outline

3.3.2. Phase 2 – Measure

The CTQ outline from the previous phase can be high in number and they might be defined as titles only. The prioritization and elaboration of CTQ outline should be studied in this phase. Especially if the SOC is providing an outsourced service, the CTQs regarding customer side should be definitely prioritized.

As it was discussed earlier, DMAIC methodology highly depends of statistical measurements. Therefore, the first step of this phase is determining what to measure and how to measure (Antony, 2006).

For a SOC team, two types of statistical data have to be studied: metrics, and maturity and capability assessment. Operational metrics, also called as quantification of security service, are the significant components of efficiency, effectiveness and satisfaction -*meaningfulness*- (Savola, 2013). Maturity and capability assessment on the other hand, is the main component to understand how processes or elements in an organization are performing (Van Os, 2016). These two items combined produce holistic data to define process capability and performance which satisfies one of the key deliverables of this phase (Aazadnia & Fasanghari, 2008).

Although the results of assessment are going to be investigated in detail in the following phase, the gaps between goals and current states are also supposed to be determined in this phase of the methodology.

Finally, the scope and goals from the previous phase should be reviewed in line with the measurement results, and objectives of the continuous improvement process should be defined (de Mast & Lokkerbol, 2012).

The deliveries should be created at this phase are;

1. Determined CTQ definitions and details
2. Process capability and performance
3. Determined gaps for improvement
4. Objectives

3.3.3. Phase 3 – Analyse

This is the phase where the results of measurement must be analyzed, and roadmap of the improvements will be created. The vital services and component of the organization should be highlighted considering the results of capability and maturity result analysis, metrics and other measurement factors if defined. One other important parameter for this prioritization is the financial quantify of the organization for improvement (Antony, 2006). The cost of required improvements for the services and components should be calculated, and prioritization of the improvement components should be re-analyzed.

Next step is defining cause-effect diagram for expected improvements. All the services in a SOC are directly or indirectly connected to each other, therefore it is not possible evaluate each of them separately and start improvement. The connectivities of different services in a SOC are described constitutively in best practices. For example, the 'Incident Handling/Response' service is directly affected by 'Threat Intelligence' service (Ruefle, et al., 2014) (Kime, 2017). On the other hand, some interactions between services or other components could vary from one organization to another. This interaction diagram should be defined, and risk assessment should be studied in order prevent possible interruptions in SOC services in the improvement phase.

Finally, considering all the parameters defined above, the roadmap of the planned improvement process should be documented.

The deliveries should be created at this phase are;

1. Prioritization of services/components to be improved
2. Determining root causes of the problems in services/components
3. Cause effect diagram
4. Financial details of improvement costs

3.3.4. Phase 4 – Improve

The components/services that will be improved are determined and planned so far and this phase is the implementation phase. Before starting implementation, risk assessment for potential problems has to be completed as the first thing. In regular DMAIC process, the implementation starts after risk assessment; however, SOC is a multi-serviced organization as it was indicated before, and doing the improvement is not an atomic action. Therefore, in this step of the methodology, another simple but effective continuous improvement approach (PDCA) has applied to this 'Improve' phase which also has its own planning, assessment, improvement and control steps.

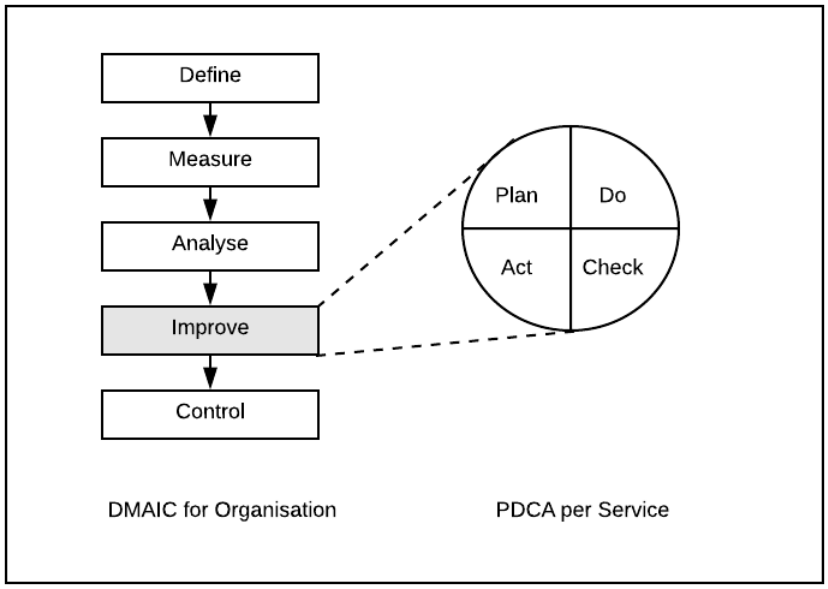

Figure 15: Applying PDCA on 'Improve' phase of DMAIC

The SOC service(s) that are the part of improvement has determined, and they will be improved by applying each step of PDCA cycle.

3.3.4.1. Plan

Similar to DMAIC, this phase includes identifying the problem that is specific to corresponding service and defining targets of improvement.

For example, recalling that our reference service is "Incident Handling/Response", a specific maturity and capability assessment could be performed to understand current status of the service (Suryawanshi, 2018) (CREST , 2018).

Another data that should be collected is the metrics related to this service. Afterwards, the results should be analyzed, and the improvement parts of the service should be determined.

3.3.4.2. Do

When the potential solution has been determined, it should be applied to a small-scale test project and results should be analyzed whether the solution has worked or not.

3.3.4.3. Check

The measurement data should be updated, and the results should be compared at this step. The first three steps of this cycle - *Plan-Do-Check*- could be assumed as an internal cycle, and it can be looped as long as necessary until the results of the improvement are satisfying.

3.3.4.4. Act

Determined solutions should be applied to all processes at this step. The results should be documented, all the relevant persons should be notified about changes and suggestions for the following PDCA cycles.

The deliveries should be created at this phase are;

1. Defining brainstorming result of possible solutions
2. Risk assessment of potential solutions
3. Defining and implementing best solutions
4. Re-evaluation of the impact of performed improvements

3.3.5. Phase 5 - Control

This is the final phase of the methodology where the results are verified, processes are adjusted in order to provide sustainability of the improvements (De Koning & De Mast, 2006). Standards and procedures have to be developed/improved align with the updates in the system, and all improvements should be documented.

The deliveries should be created at this phase are;

1. Control verification documentation
2. Standard and procedure documentation

3.4. Use Case Scenario

In this section, a use case scenario is defined to illustrate how the methodology works. The methodology includes high number of documents as deliveries which are beneficial in terms of the sustainability of the improvements; however, documentation related outputs are ignored for this use case scenario for simplicity. This defined scenario only covers data-oriented measurements and decision-making steps in the methodology.

3.4.1. Define:

The outline of the organization is defined in this step (table 4). Also, the expected maturity and capability levels for the components of the organization is defined considering budget and expectations of the project (figure 16).

Table 4: Outline of the Organization Definitions

Organization Type	- In-house
SOC Model	- Centralized
Geographic Operation	- Regional
Stakeholders	1. Security Operations Executive 2. SOC Manager 3. Cyber Security Experts
Services (Van Os, 2016)	1. Security Monitoring 2. Security Incident Management 3. Security Analysis & Forensics 4. Threat intelligence 5. Threat Hunting 6. Vulnerability Management 7. Log Management

Maturity and Capability	Target maturity (1 to 5)
Services	
1. Security Monitoring	4
2. Security Incident Management	4
3. Security Analysis & Forensics	3
4. Threat intelligence	4
5. Threat Hunting	3
6. Vulnerability Management	3
7. Log Management	2

Figure 16: Target Maturity Levels per Services for the Organization

3.4.2. Measure:

Maturity and capability assessment framework (Van Os, 2016) has been used to assess current maturity and capability levels of the organization. Results are illustrated in figure 17.

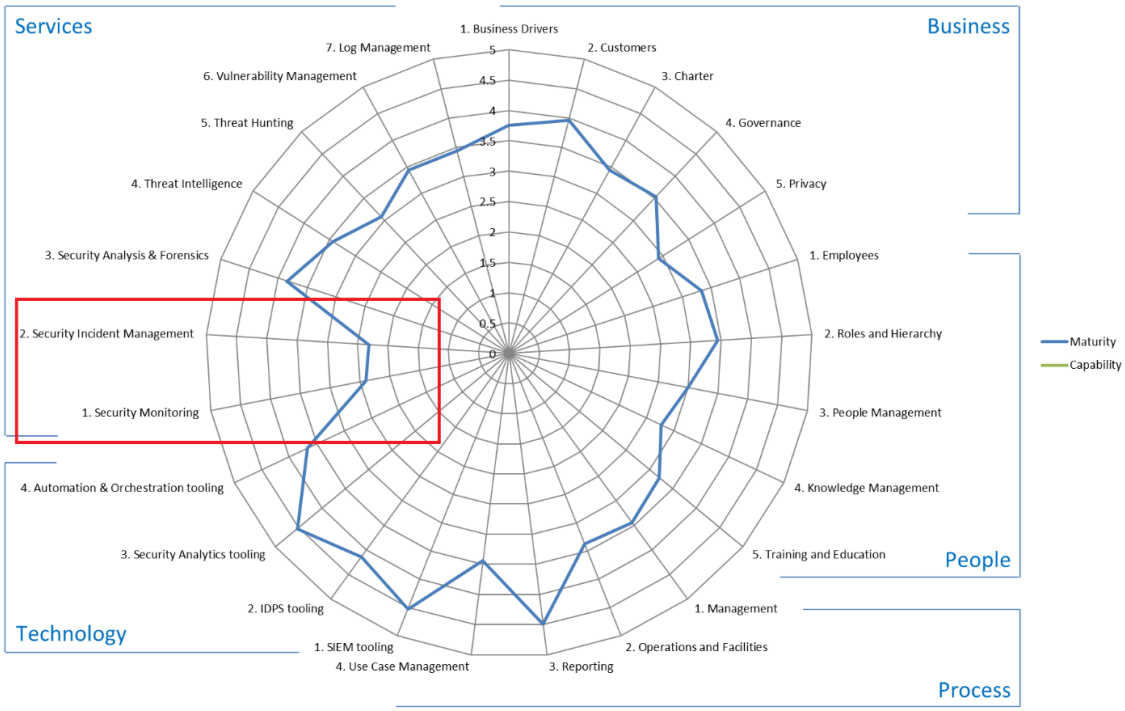

Figure 17: Maturity assessment results of the organization

3.4.3. Analyze

The results of the assessment are analyzed in this phase. In this scenario, all the services are assumed to have some score in prioritization scale, and the cost of the required improvements are ignored for simplicity. In the real cases, those parameters have to be taken into consideration as well.

Combining the expected maturity levels (figure 16) and current status of the organization (figure 17), it can be concluded that the continuous improvement must be applied to "*Security Monitoring*" and "*Security Incident Management*" firstly. These two services are complementary components of "Incident Handling/Response Service", therefore the scope is determined as improving "Incident Handling/Response Service".

3.4.4. Improve

In this step, PDCA cycle is applied to "Incident Handling/Response Service".

3.4.4.1. Plan

Similar to maturity assessment of whole organization, a more specific incident management measurement framework -*Aujas IS-IM Framework Maturity Measurement framework*- is used to understand current maturity levels of the service in terms of governance, people, process and technology (Suryawanshi, 2018).

Domains	Current	Expected
1. IS-IM Governance (Policy / Procedure/ Reporting / R&R, Metrics and Audit)	3.77	4.00
2. IS-IM Process (Process / Procedure/ Templates)	1.19	4.00
3. People (Training, Awareness, JDs/Staffing / Response arrangement)	3.25	4.00
4. Technology - Monitoring (IS-IM technology controls for detection and response/ reporting and measurement)	2.10	4.00
4. Technology - Malicious Code (IS-IM technology controls for detection and response/ reporting and measurement)	1.93	4.00
4. Technology - Network (IS-IM technology controls for detection and response/ reporting and measurement)	2.76	4.00

Figure 18: Maturity assessment results for IHR Service

The results of the detailed assessment are very similar to results of "*Security Monitoring*" and "*Security Incident Management*" maturity results in the organizational assessment in figure 17. However, this time we have a more detailed

assessment tool which will be much more useful to understand root cause of the problems.

After analyzing the assessment results, it can be concluded that the improvement should be applied to ‘Process’ category at first, then ‘Technology-Monitoring’ in the following cycle.

Taking a look at the details of ‘Process’ assessment details of the service, it can be seen that many of the items in the questionnaire is assessed as ‘0’ meaning that the organization does not have such functionality (figure 19).

DOMAIN RATING		Maturity:	1.19	
Aujas Networks - Information Security Incident Management's Maturity Assessment				
Information Security Incident Management - Maturity Assessment				
S. No.	Tool		Observations	Maturity
	The Information Security Incident Management's Process	**Source**		**2.25**
1.01	The incident management process document exists, approved by management and communicated to the relevant stakeholders	NIST 80-083	Process is document and approved by Management, however not communicated and trained to all relevant stakeholder	3
1.02	The "Incident Identification" process activity is specified	NIST 80-083	Incident identification is specified and detailed with verification and roles	3
1.03	The "Incident logging" process activity is specified	NIST 80-083	Incident logging post declaration is specified	3
1.16	Incident Management Process review procedure is in place	NIST 80-083	Periodic review, minimum once in a year is defined	0
	Incident Logging - Service Desk			**0.0**
2.01	The Service Desk function is defined for logging information security incidents	ISO 27035	Information security incidents are logged and tracked via excel sheet	0
2.02	The Service Desk is aware of their role at Tier 1/Level 1 Information Security Incident Management logging and updating status	ISO 27035	Training for categorisation / information collection and information dissemination is not provided	0
	Information Security Incident Management's Process Interactions			**0.33**
3.01	Interaction models defined for other relevant stakeholders like CERT, Management, BCP, ERT etc.	NIST 80-083	Interaction model is not appropriate with detailed R&R and notification	1
3.02	Information sharing format and template identified and documented for sharing with internal and external stakeholders	NIST 80-083	Templates were not documented	0
3.03	Integration with Change Management (post implementation reviews)	ISO 27035	Changes lead by learning's of incidents are ad hoc but follow a change management procedure	0
	Incident Records and Reporting and Communication			**1.25**
4.01	**Incident Identification** Can Incident records be created manually? Or automated	ISO 27035	Incident identification is manual	3
4.02	**Unique Reference** Does the tool automatically allocate a unique reference to newly created records at the time of opening the record?	ISO 27035	All incident have Unique reference	3
4.03	**Date and Time** Is each Incident record date and time stamped when created and again each time the record is updated?	ISO 27035	Date is mentioned and timestamp provides exact timing of the incident	3
4.04	**Source of the Incident** Does each Incident record contain a field or fields to record the identity of the source of reporting of the Incident (such as event trigger, person or group)?	ISO 27035	Source is identified	0
4.05	**Contact Details** Does each incident record contain a field or fields to record the contact information and call back method such as telephone or email?	ISO 27035	Names identified with email addressed	0
4.06	**Incident Symptoms** Does each Incident record contain a field or fields to describe the symptoms of the fault? This can include event parameters and user reported symptoms.	ISO 27035	Symptoms identified but not detailed with chronology of information security incidents	0
4.07	**Incident Status** Does the Incident record contain a field or fields to record the status of the incident (such as active, waiting, closed)?	ISO 27035	Yes, it contains the status	3
4.08	**Incident Categorization and Prioritization** Does the Incident record contain category and priority fields to record the type and impact of Incident ?	ISO 27035	Yes, with categorization and prioritization is defined	3
4.09	**Incident Assignment** Does the Incident record contain a field or field(s) to assign the incident to a support department, group or individual?	ISO 27035	Incident assignment is manual and ad hoc	0
4.1	**Incident Resolution and Closure** Do the Incident records have a field or fields to record Resolution Information including resolution date and time?	ISO 27035	Incident resolution / recovery and closure is identified as a part of procedure	0
4.11	**Management Reports** Does the tool produce reports from record detail captured?	ISO 27035	Reporting is ad-hoc	0
4.12	**Record Sharing** Does the process details the sharing of incident record and report with internal and external parties like Management, other governance bodies, CERT and Rapid Response teams	NIST 80-083	Record sharing is identified with internal and external stakeholder	0

Figure 19: Maturity assessment of process aspect for IHR

However, some of the items in the questionnaire might not be applicable to the organization. For example, in this case study, the aim could be complying all required items for NIST compliance up to expected levels, but ISO2735 compliance might not be included in organizational goals. Those values are tagged as N/A in the questionnaire for this use case scenario and final results are checked.

DOMAIN RATING		Maturity:	1.43	
Aujas Networks - Information Security Incident Management's Maturity Assessment				
Information Security Incident Management - Maturity Assessment				
S. No.	Tool		Observations	Maturity
	The Information Security Incident Management's Process	**Source**		**2.25**
1.01	The incident management process document exists, approved by management and communicated to the relevant stakeholders	NIST 80-083	Process is document and approved by Management, however not communicated and trained to all relevant stakeholder	3
1.02	The "Incident Identification" process activity is specified	NIST 80-083	Incident identification is specified and detailed with verification and roles	3
1.03	The "Incident logging" process activity is specified	NIST 80-083	Incident logging post declaration is specified	3
1.16	Incident Management Process review procedure is in place	NIST 80-083	Periodic review, minimum once in a year is defined	0
	Information Security Incident Management's Process Interactions			**0.33**
3.01	Interaction models defined for other relevant stakeholders like CERT, Management, BCP, ERT etc.	NIST 80-083	Interaction model is not appropriate with detailed R&R and notification	1
3.02	Information sharing format and template identified and documented for sharing with internal and external stakeholders	NIST 80-083	Templates were not documented	0
	Incident Records and Reporting and Communication			**0.00**
4.12	**Record Sharing** Does the process details the sharing of incident record and report with internal and external parties like Management, other governance bodies, CERT and Rapid Response teams	NIST 80-083	Record sharing is identified with internal and external stakeholder	0

Figure 20: Simplified maturity assessment of process aspect for IHR

The maturity of the service has increased from 1.19 to 1.43, but it is still below the expectations. At this step the items in the list are investigated, the missing items or the items with lower scores has been analyzed, the requirements of the improvement are determined and roadmap for improvements is created.

3.4.4.2. Do

At this stage, the improvement items have been applied to a small set of the incidents, meaning that they are applied to specific category of incidents with lower value.

3.4.4.3. Check

It has been verified that no risks or problems occurred in the processes, therefore the service specific assessment is measured again in the case of applying the improvements to whole system. The results (figure 21) shows that the maturity will be close to the expectations if the improvements can be applied successfully.

DOMAIN RATING		Maturity:	3.57	
Aujas Networks - Information Security Incident Management's Maturity Assessment				
Information Security Incident Management - Maturity Assessment				
S. No.	Tool		Observations	Maturity
	The Information Security Incident Management's Process	**Source**		**3.5**
1.01	The incident management process document exists, approved by management and communicated to the relevant stakeholders	NIST 80-083	Process is document and approved by Management, however not communicated and trained to all relevant stakeholder	3
1.02	The "Incident Identification" process activity is specified	NIST 80-083	Incident identification is specified and detailed with verification and roles	3
1.03	The "Incident logging" process activity is specified	NIST 80-083	Incident logging post declaration is specified	4
1.16	Incident Management Process review procedure is in place	NIST 80-083	Periodic review, minimum once in a year is defined	4
	Information Security Incident Management's Process Interactions			**3.50**
3.01	Interaction models defined for other relevant stakeholders like CERT, Management, BCP, ERT etc.	NIST 80-083	Interaction model is not appropriate with detailed R&R and notification	4
3.02	Information sharing format and template identified and documented for sharing with internal and external stakeholders	NIST 80-083	Templates were not documented	3
	Incident Records and Reporting and Communication			**4.00**
4.12	**Record Sharing** Does the process details the sharing of incident record and report with internal and external parties like Management, other governance bodies, CERT and Rapid Response teams	NIST 80-083	Record sharing is identified with internal and external stakeholder	4

Figure 21: Maturity re-assessment of process aspect for IHR

3.4.4.4. Act

At this stage, the planned requirements are implemented through all processes in the service. Afterwards, the maturity of the service is re-assessed using same framework.

Domains	Current	Expected
1. IS-IM Governance (Policy / Procedure/ Reporting / R&R, Metrics and Audit)	3.77	4.00
2. IS-IM Process (Process / Procedure/ Templates)	3.57	4.00
3. People (Training, Awareness, JDs/Staffing / Response arrangement)	3.25	4.00
4. Technology - Monitoring (IS-IM technology controls for detection and response/ reporting and measurement)	2.10	4.00
4. Technology - Malicious Code (IS-IM technology controls for detection and response/ reporting and measurement)	1.93	4.00
4. Technology - Network (IS-IM technology controls for detection and response/ reporting and measurement)	2.76	4.00

Figure 22: Maturity assessment results for IHR after CI

The PDCA cycle for the specific service can be re-executed many times in a loop as much as required.

3.4.5. Control

Once the improvement phase is completed, all the updates are documented, relevant persons are informed about process changes and more importantly required precautions are defined and implemented in order to make the updates permanently in the system. After the CI implementation to SOC, the final organizational assessment results are presented in figure 23.

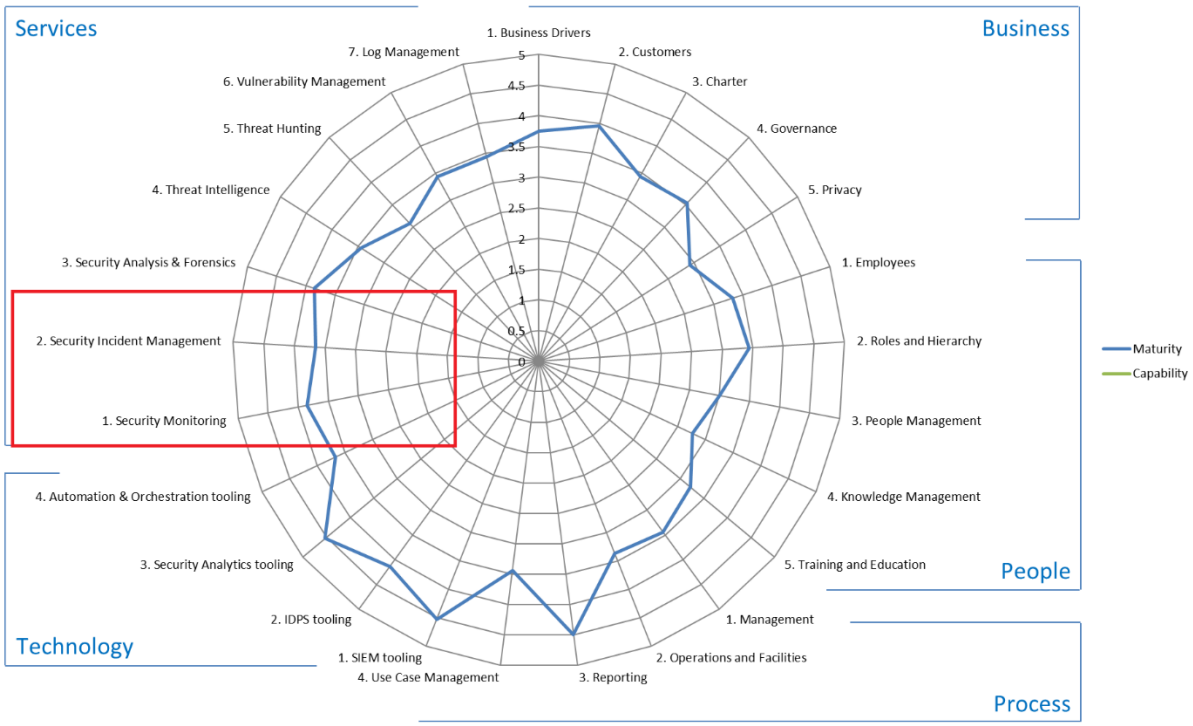

Figure 23: Maturity assessment results of the organization after CI

3.5. Summary

In this chapter, DMAIC method of six sigma, and maturity and capability assessment were combined, and a complementary improvement methodology was suggested for SOC organizations. This methodology was illustrated using a use case scenario. The use case scenario was kept simple due to the challenges such as high workload of documentation analysis requirements, and difficulty of collecting full details of an active operation center which can be classified as sensitive private information belong to theorganization. Because of such challenges, a full case study was suggested as a future work.

In order evaluate the methodology, qualitative analysis method was used, and results are reported in the following chapter of the report.

CHAPTER 4

RESULTS

4.1. Evaluation of the Methodology

In order to evaluate the suggested methodology, there is a need to better understand the perspectives and experiences of subject expert matters of cyber security domain, more specifically SOC. For this purpose, qualitative analysis approach has been used. In this context, the interviews with experienced subject matter experts were conducted, transcribed and results were analyzed using conversational analysis method of qualitative analysis approach.

Conversation Analysis (CA) is an inductive, micro-analytic, and predominantly qualitative method for studying human social interactions (Hoey & Kendrick, 2017). It is well established as a highly effective method for the investigation of interaction (Chatwin, 2014). CA does not use reduced or coded set of representations; on the contrary, it includes casual and detailed conversation details which allows the analyst to identify different perspectives and subtleties that is not realized previously. The main goal of evaluating the methodology that was suggested in this study was better understanding the perspectives and experiences of subject expert matters. Consequently, the characteristics of CA match perfectly with the goal of the analysis of the methodology.

The conversional analysis process that was performed on the suggested methodology and case study is presented under three main stages;

Subjects: The interviewee requirements were defined. The interviewees that were meeting the requirements and participated in this study were identified.

Method: Details of how the conversational analysis methodology was performed.

Results: Conversation results are analyzed, and analysis results are presented.

4.1.1. Subjects

Determining the subjects -*the interviewees*- was the first step of conversational analysis. For this purpose, following characteristics have been defined as the required qualifications of the subject candidates;

- Advance knowledge and experience in cyber security domain
- Past experience on team management or product management on cyber security domain
- Has interest on SOC processes and technologies

In accordance with these requirements, 4 subjects were determined as subjects to perform conversional analysis interview. The names and other personal information about the subjects were not shared in this report for privacy issues; however, the profile of them can be stated as follows:

- Subject-1:
    - Cyber security consultant in a global company
    - Has been managing cyber security related projects/teams for 15+ years.
    - Managed global SOC team for 5+ years.
    - Has 20+ years' experience on cyber security domain.
- Subject-2:
    - Senior executive in a cyber security-oriented company
    - Has experience in security product development management 10+ years
    - Has been working in cyber security domain 10+ years
- Subject-3:
    - Has experience on product management in a cyber security-oriented company 5+ years.
    - Has managed core technologies of SOC such as SIEM, SOAR and MDR
- Subject-4:
    - Threat hunter & Tier-3 team leader of a global SOC team.
    - Has 10+ years' experience on cyber security domain.

The subjects are mentioned via abbreviations as S1, S2, S3 and S4 correspondingly in the rest of the report.

4.1.2. Method

As a methodology, conversional analysis is largely concerned with the analysis of the verbal communicative practices that people routinely use when they interact with one another (Chatwin, 2014).

Before the interviews were performed, this study was sent to subjects and sufficient time was provided for them to investigate the methodology and use case scenario. During the interviews, although the format of the interviews was unstructured and free-flowing conversation, couple of specific questions about the methodology was determined previously and such questions were used to start and to carry on the conversation. In this way, it was ensured that conversation was not diverged from the main topic and focus point of the conversation is assured throughout the interview.

The responses were then collected, translated by the author and interpreted to make inferences.

4.1.3. Results

The results of conversations with subjects were interpreted and categorized as supportive comments and developmental comments. The supported comments were declaring that the suggested methodology is applicable, and it seems like a guiding resource for the future works in this subject as indicated by the excerpts:

S1: *"I see this approach as a promising methodology. After applying some improvements, this can be confidently used in any type of SOC organizations."*

S2: *"When a technical concern occurs in cyber security world, there is a good chance to find many resources to investigate. However, it is hard to find sufficient number of sources that focus on the management aspect of security operation teams. I think the reason is that the attack vectors are changing and improving rapidly, and security teams are using all their efforts to discover such new techniques and to adapt them. In any way, this study makes a good point as the problem it covers, and the methodology seems a guiding resource for future works."*

S3: *"Maturity assessment and security metrics are the key points for understanding and controlling SOC organization, which is the only way of improving it properly. In this connection, Six Sigma seems as a very good basis for continuous improvement process for SOC organizations."*

S4: *"This methodology seems reasonable and applicable to my opinion."*

In addition to supportive inferences, five major areas of concern were also identified by the interpretations of the interview results.

First of all, subjects S1, S2 and S4 have agreed about extending each phase of the methodology by defining roles and responsibilities of each SOC position in the CI process as indicated by the excerpts:

S1: *"Continuous improvement is a long-term and ongoing process. It includes many components, and it mostly requires the contribution of all members of the organization. If everyone in the team understands the importance of improvement process and aware of their roles and responsibilities in the process, then the success rate will be higher; otherwise, it is inevitable to face some interruptions or contingencies during improvement process."*

S2: *"In business life, unassigned tasks or responsibilities can create some problems. Many people might try to work on the same issue, or no one wants to take that responsibility. Communication among team members is very important in order to overcome such problems. But more importantly, assigning the tasks to appropriate people before starting a new process can be very useful to prevent such possible problems proactively. This methodology can be improved by adding such definitions as well."*

S4: *"I would like to understand which parts of this improvement process are in my responsibility. Which tasks should I assign to my team, and what kind of outputs will be expected from me by my managers?"*

In such way, applicability of the methodology can be increased which can result in better benefits from the improvement process.

In addition to defining roles and responsibility details, S1 also indicated that automation and orchestration has an important role in the improvement process:

S1: *"Automation is a very important concept for security operation teams. It is not always easy to answer the question 'what to automate?', but there are trending approaches or technologies that draw attention to this topic. For example, SOAR (Security Orchestration, Automation and Response) products. They aim to solve many possible problems in a SOC organization such as alert fatigue, hardship of using many security products together, communication problems or many other possible problems that I do not recollect right now. The methodology should not be focusing on improving the products or processes that currently exist, but it should be also focusing on the importance of automation and orchestration."*

SOAR platforms are increasing their popularity in security operations domain by claiming to decrease alert fatigue, which results in more available time for security analysts to focus on most important alerts in the system. As suggested by S1, the methodology can be extended with placing SOAR technology in it. In such way, the methodology -*especially the maturity assessment part*- can provide inputs to SOAR about primary automation points. In return for this, the automation processes can

increase the efficiency and effectiveness of the SOC services, which results in a mutual advantage between two concepts.

As another concern, S1 and S2 stated their concerns about the business aspect of the methodology as indicated by the excerpts:

S1: *"The scope is limited with the technical perspective of the problem. Excluding the business perspective could be very useful or misleading depending on the situation. It could be a good idea to study the same problem in business perspective in the future. In this way, the results can be compared, and the methodology can be improved."*

S2: *"As an executive, I have to think about the business side of improvement procedure as well. Extending this methodology in business perspective would provide depth to it."*

The scope of this thesis work was limited with technical aspects of the problem. The interview results showed that the business aspect of the problem could be studied in terms of improvement, and the methodology could be extended in such manner as well.

Another concern that was stated in the interviews was about simplicity of case study.

S1: *"Measuring the effectiveness and efficiency of such extensive methods is not easy. A good option would be studying a detailed case study which covers all the services in the organization including completing all challenging tasks such as implementing risk assessment or defining cause-effect diagrams."*

S3: *"I would really like to see an example of fully covered case study. It would be useful to evaluate it more easily."*

S1 and S3 has declared that a fully covered case study on an active SOC team should be performed in order to measure effectiveness and efficiency of the methodology.

Finally, S4 has stated his concerns about the service-based approach of the problems as indicated by the excerpt:

S4: *"This methodology seems to be defined with a service-based improvement approach. The interactive relations between services are already mentioned in the methodology briefly, but it could be more complicated than expected in some situations."*

Although possible effects of improving one service over other services was briefly mentioned in this study, it can be concluded that this interactive relation could create some problems during in the implementation phase. Therefore, the relationship diagram for SOC services can be created and the methodology should be reviewed by assessing such interrelationship diagram so as to prevent possible problems in implementation period.

In summary, the interviews revelated that this study provides a promising methodology for the future. It is defined by the interviewees as a complementary and comprehensive methodology which forms a basis for the future studies in this specific domain.

Additionally, the interviews also revelated that there some concerns that need to be studied as well in order to improve it. Those concerns were interpreted and presented under five main topics. The first concern was about the roles and responsibilities of SOC members in the CI process. The second was automation and orchestration of the technology core of the organization. Third concern was implementing a fully covered case study to measure the effectiveness of the methodology. Forth concern was about the business aspect of the methodology. And the last concern was about the service-based improvement approach of the methodology.

CHAPTER 5

CONCLUSION

The originality of this study is based on the presence of limited research in maturity assessment and continuous improvement practices on SOC organizations. Main goal of this study was to suggest a complementary methodology to combine both approaches by answering ‘what to improve’ and ‘how to improve’ in a SOC. For that purpose, a continuous improvement methodology in the direction of capability and maturity assessment results has been suggested.

This study can be summarized under two topics, assessment and improvement. For the assessment part, while the maturity model which was suggested by Van Os has limitations in terms of applicability to be used as a continuous improvement model, the updated version of it was suggested in this study in order to overcome that problem by offering a service-oriented improvement model. For the improvement part, DMAIC methodology of Six Sigma approach was used to provide new insight to SOC teams to detect and improve required capabilities confidently. Additionally, the methodology was illustrated with a use case scenario in order to support applicability of the methodology. Finally, the methodology is evaluated using conversational analysis methodology of qualitative analyze approach.

The evaluation results indicate that this methodology suggests a complementary and applicable perspective which can be used to increase organizational maturity. Consequently, it can be claimed that this methodology provides answers to research question of this study and it supports the hypothesis by contributing to literature.

Although the results of evaluation were in line with the hypothesis, this study has also limitations that need to be addressed in future researches. First of all, the effectiveness of the methodology was not measured in this study with quantitative data because of the difficulties in utilization of the methodology with real life scenarios. Applying this methodology to a real SOC requires high volume of sensitive information which is challenging to collect and publish. Additionally, such study requires contribution of many people in an organization, high number of meetings and documentations. Therefore, such study is defined as a future work.

Another limitation of the methodology is directly related to limitation of six sigma from the perspective of problem solving. (Antony, 2006) When defining the target maturity and capability levels of the organization, the required data which can be interpreted is collected such as budget limitations for improvement, customer expectations, CTQ definitions. However, eventually, determining the target values is still based on subjective judgement of the stakeholders.

As it was discussed in the qualitative research results, the methodology can be extended with automation and orchestration (SOAR) technologies as a future work. Brewer has noted the importance of SOAR in SOC processes and in his report the possible benefits of SOAR to importance SOC skills has been discussed. (Brewer, 2019) Additionally, Donevski and Zia has discussed using machine learning and automation to counter cybersecurity challenges, which could be a guiding paper to start studying on automation. (Donevski & Zia, 2018)

Another inference of the evaluation results was the concern about service-oriented architecture of the methodology. The scope of this study is limited with 'Incident Handling and Response' service. Separate literature research for other services in a SOC can be investigated and the methodology can be extended by defining other services. Additionally, the interrelationship diagram between SOC services could be studied and the methodology can be improved using such mapping.

As a final suggestion for future work, the methodology can be extended with defining roles and responsibilities of each position in the SOC in this CI process and it can also be improved by studying business perspective of the problem.

To conclude, although analysis results show that this study can be suggested a guiding resource for the future researches in this domain, it is important to expand further the study to establish more optimized methodology by conducting future works that are defined above.

REFERENCES

Aazadnia, M., & Fasanghari, M. (2008). Improving the Information Technology Service Management with Six Sigma. *IJCSNS International Journal of Computer Science and Network Security, 8*(3).

American Society for Quality. (n.d.). *Continuous Improvement*. Retrieved from Learn About Quality: https://asq.org/quality-resources/continuous-improvement

Antony, J. (2006). Six sigma for service processes. *Business Process Management Journal, 12*(2), 234 - 248.

Brewer, R. (2019). Could SOAR save skills-short SOCs? *Computer Fraud & Security, 2019*(10), 8-11.

Chatwin, J. (2014, 10). Conversation analysis as a method for investigating interaction in care home. *Dementia, 13*(6), 37-746.

CMMI Institute. (2017). *What Is CMMI? What Is The CMMI Model?* Retrieved 8 11, 2019, from cmmiinstitute.zendesk.com: https://cmmiinstitute.zendesk.com/hc/en-us/articles/216947067-What-is-CMMI-What-is-the-CMMI-Model-

CREST . (2018). Retrieved 7 28, 2019, from CREST - Assurance in Information Security: https://www.crest-approved.org/

CyberSponse. (2018, September 18). *5 Ways to Improve Your Cybersecurity Incident Response Plan*. Retrieved from https://cybersponse.com/5-ways-to-improve-your-cyber-security-incident-response-plan/

De Bruin, Tonia, Freeze, Ronald, Kaulkarni, Uday, & Rosemann, Michael . (2005). Understanding the Main Phases of Developing a Maturity Assessment Model. *Australasian Conference on Information Systems (ACIS)*. Sydney.

De Koning, H., & De Mast, J. (2006). A rational reconstruction of Six Sigma's Breakthrough Cookbook. *International Journal of Quality and Reliability Management, 7*, 766–787.

de Mast, J., & Lokkerbol, J. (2012). An analysis of the Six Sigma DMAIC method from the perspective of problem solving. *Int. J. Production Economics*, 604–614.

Donevski, M., & Zia, T. (2018). A Survey of Anomaly and Automation from a Cybersecurity Perspective. *2018 IEEE Globecom Workshops (GC Wkshps)*, (pp. 1-6).

Hewlett Packard Enterprise . (January, 2017). *Hewlett Packard Enterprise Report Reveals Trials and Errors of Security Operations.* Palo Alto, CA: HP Enterprise.

Hoey, E. M., & Kendrick, K. H. (2017). Conversation Analysis. In *Research methods in psycholinguistics: A practical guide.*

Holloran, D. (2018, August 24). *How to Improve Incident Management: Trust the Process*. Retrieved from https://victorops.com/blog/how-to-improve-incident-management-trust-the-process

Jacobs, P., Arnab, A., & Irwin, B. (2013). Classification of Security Operation Centers.

Judgev, K., & Thomas, J. (2002). Project management maturity models: The silver bullets of competitive advantage? *Project Management Journal, 33*(4).

Júnior, A. C., Porto, G. S., Pacifico, O., & Júnior, A. P. (2015, June 17). Project Stakeholder Management: A Case Study of a Brazilian Science Park. *Journal of Technology Management & Innovation, 10*(1).

Kime, B. P. (2017). *Cyber Threat Intelligence Support to Incident Handling.* SANS Institute.

Kwaka, Y. H., & Anbari, F. T. (2004). Benefits, obstacles, and future of six sigma approach. *Technovation*, 1-8.

Lindberg, P., & Berger, A. (1997). Continuous improvement: design, organisation and management. *International Journal of Technology Management, 14*(1), 86-101.

McAfee Foundstone. (2016). *Creating and Maintaining a SOC.* Santa Clara, CA.

Nassar, P. B., Badr, Y., Biennier, F., & Barbar, K. (2012). Securing Collaborative Business Processes: A Methodology for Security Management in Service-Based Infrastructure. *IFIP International Federation for Information Processing*, 480–487.

OWASP Security Operations Center (SOC) Framework Project. (2019, 02 21). Retrieved from owasp.org:

https://www.owasp.org/index.php/OWASP_Security_Operations_Center_(SOC)_Framework_Project

Park, C.-S., Jang, S.-S., & Park, Y.-T. (2010, March 3). A Study of Effect of Information Security Management System[ISMS] Certification on Organization Performance. *IJCSNS International Journal of Computer Science and Network Security, 10*(3).

Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014, September). Computer Security Incident Response Team Development and Evolution. *IEEE Security and Privacy Magazine, 12*(5), 16-26.

Savola, R. M. (2013). Quality of security metrics and measurements. *Computers & Security, 37*, 78-90.

Singh, B. J., & Khanduja, D. (2012). Essentials of D-phase to secure the competitive advantage through Six Sigma. *Int. J. Business Excellence, 5*(1/2).

Sokovic, M., Pavletic, D., & Pipan, K. (2010, November). Quality Improvement Methodologies – PDCA Cycle, RADAR Matrix,. *Journal of Achievements in Materials and Manufacturing Engineering, 43*(1), 476-483.

Suryawanshi, C. P. (2018, August 30). *Security Operations Center Maturity – a step-by-step DIY Guide*. Retrieved from blog.aujas.com: https://blog.aujas.com/security-operations-center-maturity-a-step-by-step-diy-guide

Van Os, R. (2016). *SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers.* Department of Computer Science, Electrical and Space Engineering. Luleå University of Technology.

Wichman, J. (2018, October 8). *3 Key Ways To Improve Your Incident Response*. Retrieved from https://www.optiv.com/blog/3-key-ways-improve-your-incident-response

Zimmerman, C. (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center.* MITRE.

TEZ İZİN FORMU / THESIS PERMISSION FORM

ENSTİTÜ / INSTITUTE

Fen Bilimleri Enstitüsü / Graduate School of Natural and Applied Sciences ☐

Sosyal Bilimler Enstitüsü / Graduate School of Social Sciences ☐

Uygulamalı Matematik Enstitüsü / Graduate School of Applied Mathematics ☐

Enformatik Enstitüsü / Graduate School of Informatics ■

Deniz Bilimleri Enstitüsü / Graduate School of Marine Sciences ☐

YAZARIN / AUTHOR

Soyadı / Surname : Erdur

Adı / Name : Efe Suat

Bölümü / Department : Siber Güvenlik

TEZİN ADI / TITLE OF THE THESIS (**İngilizce** / English) : Continuous Improvement on Maturity and Capability of Security Operation Centers

TEZİN TÜRÜ / DEGREE: **Yüksek Lisans** / Master ■ **Doktora** / PhD ☐

1. **Tezin tamamı dünya çapında erişime açılacaktır. /** Release the entire work immediately for access worldwide. ☐
2. **Tez iki yıl süreyle erişime kapalı olacaktır.** / Secure the entire work for patent and/or proprietary purposes for a period of **two year. *** ☐
3. **Tez altı ay süreyle erişime kapalı olacaktır.** / Secure the entire work for period of **six months**. ***** ■

***** *Enstitü Yönetim Kurulu Kararının basılı kopyası tezle birlikte kütüphaneye teslim edilecektir.*
A copy of the Decision of the Institute Administrative Committee will be delivered to the library together with the printed thesis.

Yazarın imzası / Signature ..... **Tarih** / Date .....