YAŞAR UNIVERSITY
GRADUATE SCHOOL

MASTER THESIS

BUILDING A SECURITY OPERATIONS CENTER WITH AN ENHANCED CYBER INTELLIGENCE CAPABILITY

KAAN ÖZYAZICI

THESIS ADVISOR: ASSOC. PROF. DR. AHMET KOLTUKSUZ

DEPARTMENT OF COMPUTER ENGINEERING

PRESENTATION DATE: 21.05.2020

BORNOVA / İZMİR
MAY 2020

ABSTRACT

BUILDING A SECURITY OPERATIONS CENTER WITH AN ENHANCED CYBER INTELLIGENCE CAPABILITY

Kaan Özyazıcı
MSc in Computer Engineering
Supervisor: Ahmet Hasan Koltuksuz, Ph. D.

May 2020,

The main objective of this thesis is to define a security operations center (SOC) with an enhanced cyber intelligence capability in order to protect organizations against cyber incidents. What are the cyber incidents and ways of it? Check the certifications and test the knowledge of staff. And check the staff classified by knowledge level or not. Types of SOC architectures while building description of SOC capabilities. Ability to calculation of SOC maturity score.

This work is intended as a roadmap to construct from scratch an advanced cyber-intelligence infrastructure fully operational cyber security operations center. The paper seeks to explain the manner in which SOC hires its workers, what SOC credentials are expected, the criteria for the SOC, the number of people in need of a SOC and how an SOC calculates the number of employees, the extent of SOC protection and the measurement of the SOC ranking.

Key words: Cyber warfare, Cyber security, Network security, Security Operation Centre, SOC, Cyber threats

ÖZET

İLERİ SİBER İSTİHBARAT YETENEĞİ İLE DONATILMIŞ GÜVENLİK OPERASYONLARI MERKEZİ KURMA

Kaan Özyazıcı
Yüksek Lisans Tezi, Bilgisayar Mühendisliği Bölümü
Tez Danışmanı: Doç. Dr. Ahmet Hasan Koltuksuz

May 2020

Bu tezin genel amacı ileri siber istihbarat yeteneği ile donatılmış güvenlik operasyonları merkezi kurmaktır. Siber Güvenlik Operasyonu Merkezinin esas amacı, siber saldırılara karşı birimleri korumak, analiz etmek ve bu saldırılara karşılık vermektir. Bu merkezin bir diğer amacı ise Bilgi İletişim Teknolojilerini gözlemleyerek hizmet sağladıkları yerlerin güvenlik birimlerini geliştirmektir. Bunun için bu birimin siber saldırılar hakkında yeterli bilgi düzeyine sahip olmaları beklenmektedir. Bu yüzden bu tezin içerisinde siber saldırılar da tanımlanmaktadır.

Siber Güvenlik Operasyonları Merkezlerinde kalifiye elemanların işe alınması ve bu işe alım sırasında onların sertifikalarının yeterlilik düzeyine göre değerlendirilip Siber Güvenlik Operasyonları Merkezi içerisindeki hiyerarşilerine karar vermek. Siber Güvenlik Operasyonları Merkezinin kurulumu sırasında gereken teknolojilerin sağlanması. Kapasitesine yani sağladıkları yeterliliklerine göre ve yönetim şekillerine göre bu merkezlerin kurulumunda kullanılacak olan mimarinin belirlenmesi. Kurulan bu Siber Güvenlik Operasyonları Merkezleri'nin olgunluk yani yeterlilik düzeylerinin hesaplanması ve bu hesaplama sırasında kullanılacak olan formül ve yöntemler bu tez içerisinde ele alınmıştır.

Anahtar sözcükler: Siber Güvenlik, İnternet Güvenliği, Siber Güvenlik Merkezi, Siber Saldırılar

ACKNOWLEDGEMENTS

First, I would like to thank my supervisor Ahmet KOLTUKSUZ for his guidance and patience during this study.

Secondly, I would like to thank to all other faculty members of the Computer Engineering Department of Yasar University.

At last, I would like to express my enduring love to my dear parents.

Kaan ÖZYAZICI

İzmir, 2020

TEXT OF OATH

I declare and honestly confirm that my study, titled "BUILDING A SECURITY OPERATIONS CENTER WITH AN ENHANCED CYBER INTELLIGENCE CAPABILITY" and presented as a Master's Thesis, has been written without applying to any assistance inconsistent with scientific ethics and traditions. I declare, to the best of my knowledge and belief, that all content and ideas drawn directly or indirectly from external sources are indicated in the text and listed in the list of references.

Kaan Özyazıcı

May 2020

TABLE OF CONTENTS

Index of Figures

Index of Tables

Symbols and Abbreviations

Artificial Intelligence	**(AI)**
Certified Ethical Hacker	**(CEH)**
Certified in the Governance of Enterprise IT	**(CGEIT)**
Certified Information Security Manager	**(CISM)**
Certified Information Systems Auditor	**(CISA)**
Certified Information Systems Security Professional	**(CISSP)**
Computer Incident Response Center	**(CIRC)**
Computer Incident Response Team	**(CIRT)**
Computer Network Defense	**(CND)**
Computer Security Incident Response Center	**(CSIRC)**
Computer Security Incident Response Team	**(CSIRT)**
Cyber Security Operations Centre	**(CSOC/SOC)**
Information and Communication Technology	**(ICT)**

Intrusion Detection Systems	**(IDS)**
Intrusion Prevention Systems	**(IPS)**
Integrated Security Operations Center	**(ISOC)**
Introduce Structured Operating Procedures	**(ISOPs)**
Information Technology	**(IT)**
Managed Security Service Provider	**(MSSP)**
Operation Systems	**(OS)**
Security Information and Event Management	**(SIEM)**
State, Local, Tribal and Territorial	**(SLTT)**

CHAPTER 1

INTRODUCTION

A Security Operations Centre (SOC) assists companies to response, prevent and identify the cyber security incidents. SOC is not just a center. It consists of people who are willing to learn and seek protection of audit. SOC has a manager who controls these people and makes arrangements with companies.

Hackers continue to grow attacks unknown and never faced against before. Nowadays almost every business and all data is in danger. Protection of the data and business's sustainability are the primary objective for growing technology era. For this manner, SOC has a very important and major role.

SOC takes a critical place on the network security services. To provide the security, SOC staff must be qualified and certified by the authorities such as EC-Council, SANS and CISCO. Selection of the qualified personnel is a critical role in SOC because in some cases staff should use manually scanning techniques instead of autonomous tools. Every SOC have a maturity score and the score is calculated by their capabilities.

This thesis aim is to be a guidance to build a fully operational cyber security operations center with an enhanced cyber intelligence capability. This thesis also strives to be an answer for how SOC hire its personnel, what qualifications are needed by SOC, what capabilities are obligatory in the SOC, how many people does a SOC need and how does a SOC decide the amount of personnel, what SOC security score and how SOC score can calculate.

CHAPTER 2

LITERATURE REVIEW

This thesis references to some previous researches, brochures of companies providing SOC service and roadmaps of some organizations which are authorities in network security area.

(Torres A., 2015) defined that triad of Security Operation Center (SOC). What is people, process and technology. What are the SOC duties and which trainings do SOC staff need. How can SOC decide job title for the crew? When approaching the challenge to create a SOC, the ability to predict mutual challenges would make it easier to start up, develop and grow over time. According to capabilities and effectiveness they proposed a way of scoring scheme for the SOC. And they aimed to improve the SOC capabilities and efficiencies. (EPRI, 2013) This research reflects on the early steps in the process to set up an ISOC (Integrated Security Operations Center): business case creation, future organizational issues, trade-offs with multiple ISOC models, and implementation preparation. The findings are based on current research, contribution to infrastructure and a study of ISOC applications outside the electrical industry. (Zimmerman C., 2014) This book presents ten effective CSOC (Cyber Security Operation Center) techniques regardless of their scale, capability or form of constituency. The methodology in particular, and how individuals, structures and technology cross-cut components. They discuss in depth different CSOC fields, starting from the number of analysts a CSOC needs to determine where the sensor technologies are located. SOCs are a critical service for companies who want enforcement and the monitoring of threats. While there are mechanisms that address the technology aspects of these programs, there is currently no comprehensive structure that covers procedures, personnel, and technology. In addition, it will be useful for organizations and stakeholders contemplating the development, procurement or sale of such facilities to assess the efficacy and quality of the services offered. In this paper (Jacobs P., et al, 2013), suggest a ranking and classification scheme for SOC services, assessing both the capabilities and the maturity of the services given. In many organizations, owning a SOC, only a few of them are actually successful in counteracting cybercrime and IT misuse. A method of calculation was developed to determine the efficacy of the defense offered by a SOC (Schinagl, et.al.,2015). By the light of these papers and researches this thesis can be efficient roadmap for those who wants to build a SOC.

CHAPTER 3

CYBERSECURITY

3.1 What Is Cybersecurity

Cybersecurity is largely around people processes and technology working together to cover the full spectrum of threat reduction, risk mitigation, prevention, external cooperation, reaction to events, resilience and recovery strategies and practices, including computer network activity, information assurance and law enforcement ("Cyber security introduction," n.d.).

Cybersecurity protects internet-connection based systems such as, hardware, software and data against cyber incidents. It is composed of two terms, one being cyber and the other being secure. Cyber is the infrastructure that includes structures, networks, services, or records. Whereas security relates to safety that involves security of the infrastructure, security of the network, device and details ("Cyber security introduction," n.d.).

It is a set of technology, procedures and activities designed to protect networks, computers, systems and data from threats, abuse, harm, intrusion or unauthorized access. It may also be related to as security of information technology ("Cyber security introduction," n.d.).

Cybersecurity can be described as a set of policies and standards aimed at protecting our critical and online information from threats. Due to the heavy reliance of technology in a modern industry that stores and transmits an array of sensitive and vital information about people, cyber security is a critical function and many companies require insurance ("Cyber security introduction," n.d.).

3.2 Why Is Cybersecurity Important

In a digital world that recognizes that our private information is more sensitive than ever before, we now reside in a networked environment, from internet banking to government infrastructure, where data is stored on computers and other apps. Some of these may include sensitive data, including intellectual property, financial data, personal data or any other form of data which could have negative effects, such as unauthorized access or disclosure ("Cyber security introduction," n.d.).

Cyber-attacks are now a worldwide issue and have raised several questions over hacking and other cyber breaches able to threaten the global economy. In order to protect the knowledge and technologies used to handle it and archive it, organizations are exchanging sensitive data through networks and other tools during the course of enterprises ("Cyber security introduction," n.d.).

As cyber-attacks become increasingly frequent, enterprises and organizations, namely those that provide information relevant to the protection of their sensitive business and personal information on national security, health and financial information, are required to take measures ("Cyber security introduction," n.d.).

3.3 Aim of Cybersecurity

The aim of cybersecurity is to defend against theft, hacking or attack. There are three major goals of cybersecurity,

1. Confidentiality
2. Integrity
3. Availability

Figure 3.1 CIA Triad

In addition to CIA Triad, there are some other concepts of cybersecurity. Such as, Audit.

The CIA triad most businesses and organizations use when a new application is built, when a data database is created, or when access to certain data is guaranteed. All these safety goals must be implemented in order for data to be fully secure. These are both co-operating defense measures and cannot be as effective if one is ignored (“Cyber security introduction,” n.d.).

3.3.1 Confidentiality

Confidentiality is about as equal to anonymity which prohibits unwanted knowledge release. It includes data protection and provides access. It prevents important information from reaching the wrong people while ensuring that it is received by the right people (“Cyber security introduction,” n.d.).

Confidentiality tools can be listed as encryption, access control, authentication, authorization and physical security.

- Encryption

Encryption is a data processing process that is unreadable by an algorithm to unauthorized people. A secret key (encryption key) is used to transform the data so that transformed information can be read only by using another secret key (decryption key). It protects sensitive information such as number of credit cards by encoding and converting data into text that is not understood. Only by decrypting this encrypted data can be read. The two primary types of encryption are the asymmetric and symmetric keys.

- Access Control

Decides rules and policies to restrict access to a system or physical and virtual resources. It is a process through which users have access to systems, resources or information, and certain privileges. Users may provide authentication in access control systems before they can enter, such as name of an user or a serial number of their machine. Such credentials in physical systems can take many forms, but the most protection is passwords not transferable.

- Authentication

A method of authentication guarantees and establishes the identification or function of a customer. Authentication is a must for all businesses, as it allows organizations to safeguard their

networks by allowing authenticated users only to access their protected resources. Such tools may include computer systems, networks, repositories, websites and other network software or facilities. Those resources are available.

- Authorization

Authorization is a security mechanism that allows or has something to do. This is used as the basis of access control policies, including computer programs, files, services, data and app features, to determine a person or system. access to resources. Authentication is usually preceded by a user identification test. System managers are typically approved for all programs and user services. Throughout authorization, a program tests the access rules of an authorized user and permits or refuses access to the property.

- Physical Security

Physical security explains steps to prevent unauthorized access to IT assets such as infrastructure, facilities, critical information, resources and other damage-related properties. It protects these assets, including theft, vandalism, fire and natural disasters against physical threats.

3.3.2 Integrity

Integrity refers to the techniques used to ensure that data is real, accurate and protected against unauthorized user changes. This is a property which does not alter information unauthorized and which is a genuine source of information (“Cyber security introduction,” n.d.).

Integrity tools can be listed as backups, checksums and data correcting codes.

- Backups

Backup is a regular data archive. It is a process of copying data or data files to be used for loss or destruction of the original data or data files.

- Checksums

A checksum is the number type used to validate the completeness of a data file or transfer. In other terms, a method is calculated to convert the file's contents to a numerical value.

- Data Correcting

It is a form of data storage in order to detect and periodically fix small changes.

3.3.3 Availability

Availability is the property that allows the authorized persons to access and modify information in a timely manner. It ensures that authorized individuals can reliably and continuously access our sensitive data (“Cyber security introduction,” n.d.).

Availability tools can be listed as physical protections and computational redundancies.

- Physical Protections

Physical safety enables the availability of details even when physical challenges emerge. This offers secure housing for sensitive information.

- Computational Redundancies

It is extended as an accident fault tolerant. It prevents machines and storage devices which are used to restore failures.

3.3.4 Audit

Audits are the more reliance activities. They are main methods for verifying accordance. It is a measurement of an organization or product against a specific standard to formally validate that the exact needs are fit. There are two types of audits, external and internal.

- External Audit

  The information security status of the company shall be measured against a defined standard, both auditable and certifiable. ISO / IEC27001 is a leading Standard that is both auditable and certifiable. Using this standard an authorized auditor will review the information security role of the company to ensure that the organization meets the requirements set out in the standard. Specifications include aspects of mandatory measures that must be adhered to, documentation of processes and procedures that must be implemented and adequately communicated within the company and continuously enforced. When the company effectively shows compliance with this requirement and passes the certification evaluation process is the probable next step. Certification is generally valid only for a set duration, during

which an entity must again demonstrate compliance in order to maintain its certification. This ensures that the safety is maintained continuously and that the certification can maintain its value and recognition. And an audit will involve regular visits to verify that the specifications continue to be enforced successfully over the long term.

- Internal Audit

An internal audit can help determine the degree of the organization's compliance with a specification's specifications or establish a benchmark for evaluating progress for future audits. Internal audits are often carried out as the practice runs before an external audit. It's important to note that while audits may provide such evaluations such as gap and risk assessments as part of their process, an audit and an evaluation are not the same. An evaluation can be performed internally and can cover one specific field, while an audit takes into account all aspects of the protection of an entity and is often undertaken by an independent professional. An audit is to validate the outcome is usually a pass or fail.

Audit is needed when the external audit is mostly carried out to comply with the various regulations of the industry. As a trusted organization, you have probably designed and applied cybersecurity policies, communicating and educating your employees about them and ensuring that these practices and policies are continuously revised and maintained to ensure that the digital assets you process are protected at all times.

The safety audit provides a special degree of assurance. It is a means of checking and validating the application of what you have documented in your policies, and of checking that you have enforceable controls in place to ensure that your policies are continuously applied correctly throughout your organization. When an audit assesses compliance, it also identifies areas of non-compliance and where the specifications of the standard have not been properly met. In this case, solutions can be provided so that changes can be made and more restrictions can be added in order to satisfy compliance.

CHAPTER 4

CYBER INCIDENTS

A computer system and network are being used as a cyber-attack. This utilizes malicious code to modify computer code, logic or details, contributing to cyber-crimes such as identity theft and knowledge.

Many citizens now use computers and the internet. When digital issues are focused, criminal code activities are rising and evolving like any type of crime. As described in ("Types of cyber attacks" n.d.) Under two groups cyber-attacks may be classified.

1. Web-based Attacks
2. System-based Attacks

4.1 Web-based Attacks

These kind attacks take place on a website or on web applications. Several of the major web-based attacks are defined in the below ("Types of cyber attacks" n.d.)

4.1.1 Injection Attacks

It is the attack in order to manipulate the application and obtain the information required in a Web application. For example, SQL Injection, code injection and log injection are the well-known injection attacks.

4.1.2 DNS Spoofing

DNS Spoofing is a kind of encryption manipulation of a computer. What happens to the data in a DNS resolution cache that leads to an incorrect IP Address from the name server which transfers traffic to the attacker's computer or any computer other than that. DNS spoofing attacks can occur without being identified for a long period of time and can cause serious security problems.

4.1.3 Session Hijacking

This is a vulnerability assault on a secured network personal session. Cookies are generated by web applications to store the state and user sessions. An intruder can control all user information by stealing cookies.

4.1.4 Phishing

Phishing is a type of attack aimed at grabbing sensitive information such as user username and card number. This takes place when an intruder hides itself in electronic communications as a trustworthy individual.

4.1.5 Brute Force

It is a type of attack that uses a method of trial and error. This assault produces and validates a large number of conjectures to extract real information, such as user password and identification number. The assault is used to crack encrypted data by criminals or by safety analysts to test the network security of an organization.

4.1.6 Denial of Service

An assault that is intended to prevent users from using a computer or network tool. This is done by overwhelming the target with traffic or sending information that triggers a collision. The same device and internet connection are used to attack a server.

4.1.7 Distributed Denial of Service

A DDoS-attack is an attempt to disrupt normal traffic by overwhelming the target, or its surrounding infrastructure by a flood of Internet traffic, from a targeted server, service, or network. By using various computer systems as sources of attack information, DDoS attacks gain effectiveness.

4.1.8 Dictionary Attacks

This type of attack saved the standard password list and checked it in order to have the initial password.

4.1.9 URL Interpretation

It's a type of attack where you can modify some bits of an URL and you can build a web server for which you can't search web pages.

4.1.10 Man in the Middle Attacks

It is a kind of assault that allows an attacker to intercept and act as a link between communications between clients and servers. This will enable an intruder the data in the intercepted link to be interpreted, extracted and changed.

4.2 System-based Attacks

These attacks aim to compromise a computer or a network of computers. System-based attacks are listed in below (“Types of cyber attacks” n.d.).

4.2.1 Virus

This is a form of malicious software which is distributed in all computer files without a user's awareness. It is a malicious program that replicates itself when it is implemented by inserting copies in other computer programs. It can also execute commands that destroy the device.

4.2.2 Worm

A type of malware that primarily replicates to uninfected computers. it is a malware type. It works like the virus of the machine. Worms also arrive from email attachments from trustworthy senders.

4.2.3 Trojan

It is a malicious program that results in unexpected computer changes and unusual activity, even if your computer is idle. It fools the consumer with his true purpose. It seems a simple program, but some malicious code can run in the background when it is opened / executed.

4.2.4 Backdoors

It is a tool that eliminates the normal process of authentication. An attacker can create a backdoor for a problem-solving application or operating system to access.

4.2.5 Bots

An automated bot mechanism connects with the other systems on the network. Many programs run continuously, while others only execute commands when particular inputs are received. Crawler, chatroom and destructive bots are common examples of the Bots.

CHAPTER 5

SECURITY OPERATIONS CENTER (SOC)

5.1 What Is SOC?

Security Operations Center is a centralized unit that deals with cyber security issues of an organization. SOC performs as a group of skilled people with defined processes and supported by integrated security intelligence technologies. It is a center that consist of network security analysts who monitor the ICT systems. The SOC focuses specifically on cyber threat, monitoring, forensic investigation, and incident response and reporting, below the scope of a general environment for security operations with consistent strategic support. At the end the main goal of a Security Operations Centre is to improve security of an organization by monitoring ICT (Information and Communication Technology). In other word a SOC can be described as a team contains system analysts and engineers. This highly skilled team monitor the network 24/7 and 365 days. SOC, protects the organization against to cyber threats and responds. The SOC especially focuses on cyber threat, monitoring, forensic investigation, and incident management and reporting (Torres, A., 2015).

A SOC can be named as in the below (Torres, A., 2015),

- Computer Security Incident Response Team (CSIRT)
- Computer Incident Response Team (CIRT)
- Computer Incident Response Center (CIRC)
- Computer Security Incident Response Center (CSIRC)

At the end, all of the above teams and centers evolve into SOC by becoming a part of it. SOC identifies itself as people, process and technology. In Figure 5.1 shows triads of a SOC. In the end, SOC comes up with three aspects and these are people, process and technology.

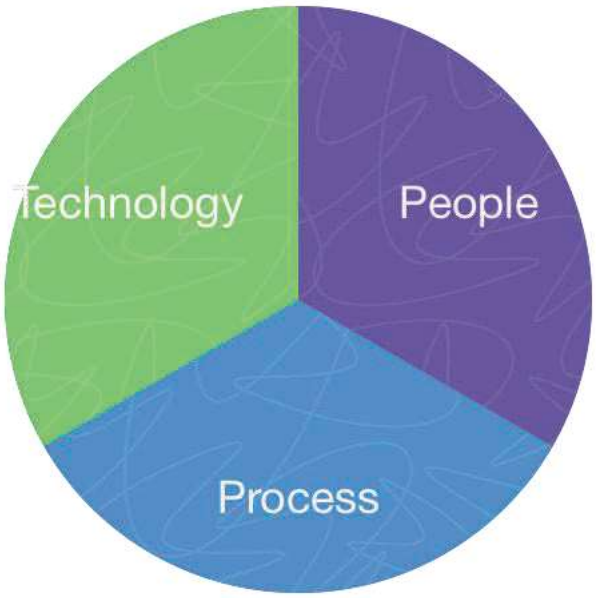

Figure 5.1 Triad of SOC

5.1.1 People

SOC team must be well trained because a SOC is as good as only its people. This team monitors and defense against forbidden activities within computer networks. The SOC staff must have proficiency in computer network defense (CND), operation systems (OS), network protocols, multiple hardware platforms, Routers, Switches, Firewalls, programming, databases, forensics, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). SOC staff should be expertly analyze a variety of data. The SOC unit's main purpose is to aid, coordinate and report on cyber incidents effecting State, Local, Tribal and Territorial (SLTT) governments. Required qualifications of the SOC organization is shown in Figure 5.2. SOC staff consist of four job title (Torres, A., 2015). These are,

1. Tier 1 Alert Analyst
2. Tier 2 Incident Responder
3. Tier 3 Subject Matter Expert / Hunter
4. SOC Manager

- Tier 1 Alert Analyst

These staff must continuously monitor network and health of security sensors and endpoints prioritize the security alerts. Collects sensitive data to transfer to Tier 2. These are the duties of

the Tier 1 SOC Alert Analysts. On the other hand, intrusion detection, network security, TCP/IP Protocols, SQL, host-based inquisitive training, security information and event management (SIEM) and the rest of the tool-based trainings are the requirements of the Tier 1 SOC Alert Analysts. Some certifications are obligatory. Such as, CEH, CND, SANS certificates and some other certificates (Torres, A., 2015).

- Tier 2 Incident Responder

SOC Tier 2 Incident Responders must perform deep-dive incident analysis by gathering and correlating the data from different sources and after examining, decide if it is harmful or not for the systems. If critical systems and data are damaged, search for new analytical methods and apply them into the detecting threats. Compared to Tier 1 Analyst, Tier 2 Incident Responder must have more advanced knowledge of network forensics, host-based forensics, incident response procedures, logging, basic malware detection and threat intelligence. Tier 2 stuff also must have the certificates Tier 1 have. In addition to Tier 1 certificates, SANS Hacker Tools, Techniques, Exploits and Incident Handling and Advanced Security Essentials certificates are looked for (Torres, A., 2015).

- Tier 3 Subject Matter Expert / Hunter

SOC Tier 3 Subject Matter Experts have in-depth knowledge on network, endpoint, threat intelligence, forensics and malware analyzing. In addition to these, SOC Tier 3 Subject Matter Experts have deep understanding of IT infrastructure, anomaly detection and threat intelligence. The expecting certificates are about Penetration Testing, Reverse Malware Engineering, Intrusion Detection and Exploiting Techniques (Torres, A., 2015).

- SOC Manager

SOC Manager operates personnel, budget, shift scheduling and technology strategy. It performs as an organizational end point for the crucial business incidents and has overall control for SOC. SOC Manager is responsible for computing and arranging resources with the aim of detecting, investigating and mitigating incidents that could influence the business. The SOC manager will create a process model and introduce structured operating procedures (SOPs) to direct analysts through triage and response protocols for the incident handling process. Project management, incident response management and people management are demanded skills for the SOC Manager. Also, CISSP, CISA, CISM or CGEIT certificates are obligatory (Torres, A., 2015).

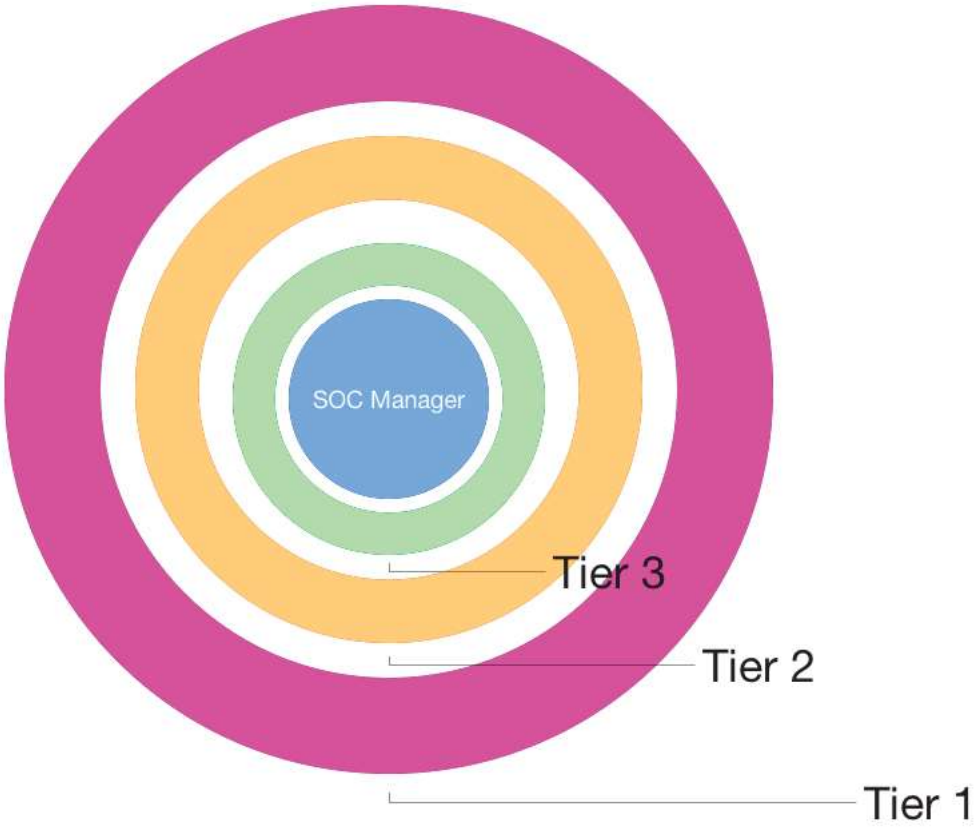

Figure 5.2 Organization of SOC

5.1.2 Process

The SOC also needs to perform advanced forensic analysis on objects such as hard drive images or full-session packet capture or malware reverse engineering on malware samples collected to assist an incident in order to determine the nature of the attack. Sometimes it is important to collect and analyze forensic evidence in a legally sound way. The SOC must be more rigorous and repeatable in its procedures in such cases than would otherwise be necessary. SOC workflow model is shown in below in Figure 5.3. (Torres, A., 2015).

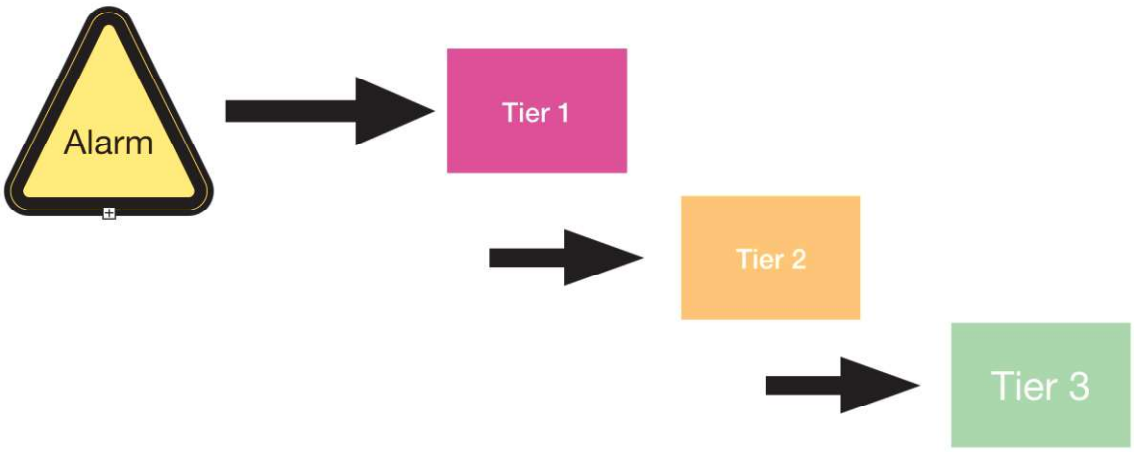

Figure 5.3 SOC Workflow Model

Defining repeatable triage of events and review procedures formalize a SOC analyst's activities to ensure that no significant duties take advantage of the system. By designing repeatable crisis response process, the roles and activities of team members are established from the formation of a warning and initial Tier 1 assessment to Tier 2 or Tier 3 personnel escalation. According to the SOC workflow, resources can be efficiently allocated. The most popular incident response process model is the DOE/CIAC. In NIST 800-Series (Dempsey et al., n.d.), this model consists of six stages: preparation, identification, containment, eradication, recovery and lessons learned.

5.1.3 Technology

A SOC must be built with a range of technology products that provide the correct environmental awareness in accordance with the security position of the company. The SOC must appoint a professional security detail while selecting the right technologies to identify exactly which resources are right for the job (Torres, A., 2015).

Some of the tools required may include technology for intrusion detection and prevention; SIEM systems; software for handling danger and vulnerability; filtering technologies; tools for data loss prevention; solutions for traffic / packet inspection; frameworks for data analysis; and technologies for monitoring. Furthermore, based on the extent of the duties, the SOC may also have links to other business systems such as investigative technology software that support efforts to evaluate incident response (Torres, A., 2015).

Though technological solutions are essential, development delivery is expensive and inefficient for the sake of technology. SOC implementation initiatives should first evaluate what is accessible in-house to satisfy SOC needs: by adding new tools and technologies, the SOC can then improve and extend current capabilities.

The essential technologies used in SOC are shown in in the Figure 5.4. In section 5.3, SOC technologies and capabilities described in detailed (EPRI, 2013).

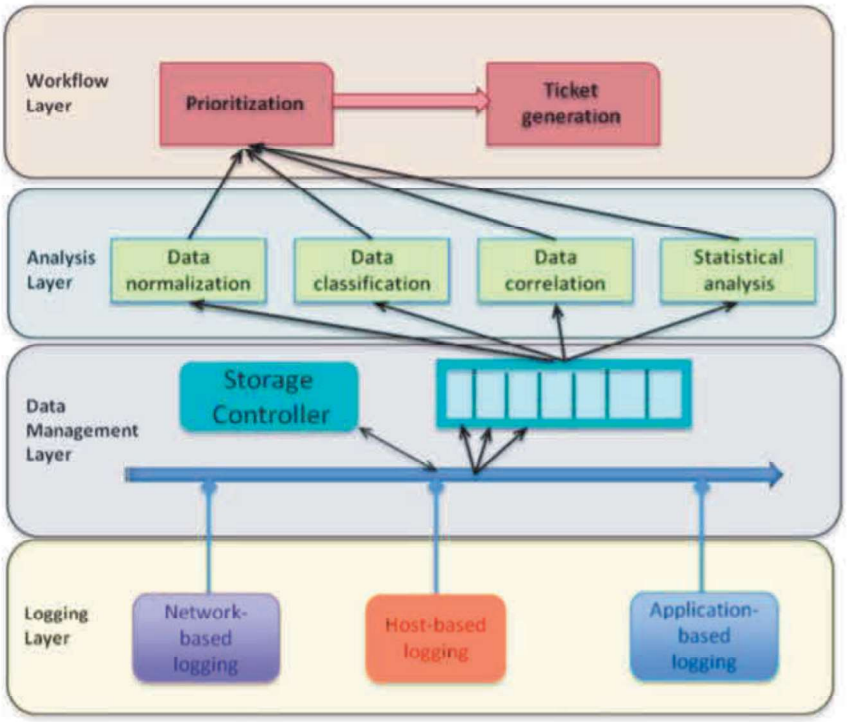

Figure 5.4 Technologies used in SOC (EPRI, 2013)

In Figure 5.4 technologies grouped into four categories:

1. Logging
2. Data management
3. Analysis
4. Workflow

- Logging

The purpose of the logging layer is to include the basic coverage required to drive the SOC analysis. Ideally, an SOC would gather the limited piece of information needed to cover events occurring within a service, but as additional data sources are available, it should be able to

seamlessly provide them. The nature of logging applications and the extent of their capabilities can differ (EPRI, 2013).

Network-based Logging

Network traffic monitoring tools are built to measure the efficiency of the network's inbound and outbound contact flows. To collect details such IP addresses, ports, etc., session layer audit reports and overall network management information, the logging layer may include many typical network sensing devices. Forward event generation applications include anti-virus, malware detection, IDS and IPS.

Host-based Logging

Techniques for network tracking record privilege-escalation behavior, log degradation, and internal server operation. However, these internal activity sensors are subject to increasing attacks themselves, likely to result in the security service being disabled or completely removed. Consequently, in addition to host-based logging applications, network-security deficiencies could be identified by more sophisticated event generation applications that track host sensor actions. Applications aimed at preventing data loss are also applicable at this point.

Application-based Logging

Applications are used at the source code or binary stage on this layer. Advanced technologies are available that receive these skills and generate information about logging. Given the highly critical delivery setting of control systems, where resource constraints are also in effect, host-based and application-based logging may not be sufficient.

- Data Management

There are two main roles in the data management system: first, to distribute data from the logging layer, and second, to efficiently store data. Both procedures must be performed in a safe manner. Various systems can be used to process data, based on whether the SOC has real-time functionality or whether unified or hierarchical model is used. Certain considerations must also be addressed, such as data normalization for stable semiconducting and data duplication minimization across network links to facilitate scalable selection. At this point, it is possible to filter data further and save only the relevant information (EPRI, 2013).

There are two forms of design that can be used:

- A centralized approach –data is compiled, processed and evaluated in a central location. This method is ideal for specifications with non-real-time scalability and more versatility.
- A distributed approach -using distributed file systems to store data. This method is ideal for criteria for greater scalability. Nevertheless, if real-time criteria are needed, data can be processed as a medium, while storage systems are used only for forensic analysis. In this scenario, assistance must be received in real time by the data distribution system.

- Analysis

When data is collected, it is analyzed by the analytical layer to identify specific security case. Some SIEM systems are based on one or more of the following computational activities:

- Data normalization - provides a standard framework for network, host and device data collection, allowing for further textual study.
- Data classification - provides a description of the various events according to their terminology.
- Data correlation - provides tools beginning with limited flexibility in terms of the forms of IT-related events. Correlations can also take physical and conceptual location information into consideration. Technologies will develop into more advanced capabilities to identify multi-stage assaults.
- Statistical analysis - extends the ability to correlate with more statistical analysis of the three-level events, operating over time and space (multiple devices) to detect more relevant events.

- Workflow

When cyber incidents are created, priority is given to taking action. Cyber incidents are usually given priority based on business relevance. These can also be graded to be overcome depending on the requisite technical skills. SOC supporting technologies also need to allow functioning tickets to be dispatched. Popular ticketing systems provide customized configuration capabilities that can be adapted to specific procedures. Most enterprise protection management packages also include workflow tools that allow monitoring of cyber incident response (EPRI, 2013).

5.2 Why Do We Need a SOC?

Information security's importance is rapidly increasing. Cyber-attacks are matter of 'when' instead of 'if'. Organizations are continuously under attack from hackers and the other suspicious actors. Companies are expeditiously becoming more vulnerable to cyber-attacks. The main reason is, companies or organizations spend less importance on the IT and better information security. Cyber incidents always occur. No organization is safe. Every system, network, organization, infrastructure and application can be attacked or hacked. Vulnerabilities always exist in organizations. According to Yücesoy and Pazoğlu, "the realization of penetration by attackers to any given computer system is about 320 days. External notifications take 140 days, but the internal discovery takes 56 days." (Yücesoy and Pazoğlu, 2019). If the damage is measured it will be seen that it amounts to some values with six digits numbers. SOC aids almost every size of organization.

SOC maintains the organization running, keeps health of the business harmless. SOC also prevents the loss of sensitive data and monitors user activity, collects external or internal threats. Companies should advance their protection and detection in order to respond to the cyber incidents. No organization or company is fully protected against cyber-attacks. Number of attackers grows every day and attackers become more vicious. According to Zimmerman (2014, p.41), the operational time lapse of the attacker versus the defender comparison described in the below.

In years, attackers derive new ways of attacks. Defenders bring into practice new defense strategies. Collect and incorporate financing, interaction and delivery of technology for a new SOC.

In months, attackers build participant script kiddies teams or thousands of "bots" capable of attacking multiple large corporations. Carry out a whole campaign of interference against a big, complicated goal such as a Fortune 500 corporation or a government agency. By the way, defenders recover fleets of the network or host sensor. Complete instrument a tracking data center. Recruit and train IT experts as Tier 1 CND analysts. Enabling policy documents and authorities to write, socialize, finalize and register.

In weeks, attackers perform comprehensive reporting on an individual that is targeted. Defenders develop, deploy and render custom detection and analytics tools like Perl scripts and SIEM use cases that are complex to run. An internal SOC standard operating procedure (SOP) is checked, reviewed, and baseline.

In days, attackers list and take over a whole company thoroughly. Weaponization into an attack vector of a patch update. Defenders review all signatures deployed to an IDS fleet or content deployed to SIEM on a monthly / quarterly basis. Testing and moving a big patch for a product. The quality of a hard drive picture from a device involved in a serious accident is analyzed and recorded. Evaluate an adversary's actions and possible motivations and goals on constituent networks.

In hours, attackers try to escalate privileges to admin. Defenders create or import IDS signatures and deploy them to a sensor fleet. Identify, assess and build a response plan for multiple systems or accounts experiencing an intrusion. Provide cursory payload analysis for a new malware strain. Identify and recover from a sensor or data feed that is down. Gather stakeholders and update them on the specifics of a current major incident.

In minutes, attackers phish is a large user community of the product. Establish a presence on a host that is kept secret. Exfiltrate from main assets targeted confidential data. By the way the defenders request the log data for any device in an organization for each month and collect information. Retrieve a week worth of indexed PCAP for a given set of IP addresses from online storage. Recognize and tag an incident of concern as benign or fill out a case and escalate it to Tier 2. Isolate a host that is tainted. Identify and notify a sysadmin at a site with a possible incident involving the device.

In seconds attackers commit a host by installing drive-by or remote service. Skip from one IP or domain step-by-step to another, bypassing IP block lists. Morph unique code of attack, thus circumventing IDS based on signatures. Exfiltrate from a website or network exchanging a handful of highly sensitive information. Defenders prevent an attack on the network or host automatically by means of a security device such as HIPS. Generate and submit an audit entry

to a SIEM console. Activate an IDS alert and send the message to the SIEM console as well as the corresponding packet.

Can organizations deal this kind of attack speed without a SOC? No, they can't handle with these kinds of attacks. Even if they can, there are still differences between how quickly the attacker can move and how quickly the defender determines how best to respond. SOC takes advantages in this stage for better security. That is why organizations need a SOC.

5.3 SOC Capabilities

A SOC addresses the network management and security needs of the community by delivering a set of services. The changing threat environment has made the latest technology significantly necessary in CND operations. According to Zimmerman (2014, p.18-24), SOC capabilities described under eight categories in the below,

1. Real-Time Analysis
2. Intel and Trending
3. Incident Analysis and Response
4. Artifact Analysis
5. SOC Tool Life-Cycle Support
6. Audit and Insider Threat
7. Scanning and Assessment
8. Outreach

5.3.1 Real-Time Analysis

SOC provides real-time analysis for businesses. This capability divides into two. These are Call Center and Real-Time Monitoring and Triage.

- Call Center

Advice, reports of incidents and requests for CND services from constituents obtained by phone, email, updates to the SOC website or other forms. This is roughly equivalent to a conventional IT help desk, except that it is unique to the CND.

- Real-Time Monitoring and Analysis

Triage and quick monitoring of real-time data streams for possible intrusions (such as device logs and alerts). Suspected cases are escalated into an incident investigation and response team for further review after a specified time threshold. Normally identified with Tier 1 analysts from a SOC, concentrating on events real-time feeds and other visualizations of results. This is one of the SOC's most easily recognizable and measurable capabilities, but without a corresponding incident detection and response capability, it is worthless.

5.3.2 Intel and Trending

This caption divides into six and these are,

1. Cyber Intel Collection and Analysis
2. Cyber Intel Distribution
3. Cyber Intel Creation
4. Cyber Intel Fusion
5. Trending
6. Threat Assessment

- Cyber Intel Collection and Analysis

Collecting, processing, and reviewing computer intelligence reports, malware breach studies, and information security articles reporting new threats, exploits, devices, and study. Products are examined for knowledge that involves an SOC response or shipment to the electoral district. Knowledge can be derived from the cooperation of SOCs, vendors, blogs of news media, online forums and lists of email distribution.

- Cyber Intel Distribution

Synthesis, review and dissemination of cyber intelligence reports, cyber-attack alerts and information security news to constituent members perhaps on a routine basis (such as a weekly or monthly cyber newsletter) or on a non-routine basis (such as an emergency update or phishing activity alert).

- Cyber Intel Creation

Key authorship of new articles on cyber security, such as vulnerability alerts or high points, focused on the SOC's primary research. Analyzing a new threat or weakness not seen before,

for example. This is usually driven by the SOC's own incidents, forensic analysis, analysis of malware, and commitments to the adversary.

- Cyber Intel Fusion

Extracting and synthesizing data from cyber intelligence into new signatures, information, and comprehension of adversary TTPs, while changing surveillance operations.

- Trending

Long-term feed monitoring of incidents, captured malware, and incident data for evidence of disruptive or suspicious behavior or for better understanding of constituent or adversary TTPs. This may include unstructured, open-ended, deep-dive analysis of different data sources, pattern and association over weeks or months of log data, "low and slow" data analysis, and advanced techniques for identifying anomaly.

- Threat Assessment

Holistic assessment of threats posed by different actors in the cyber domain against the electoral district, its enclaves or business lines. This will include leveraging existing resources such as cyber intelligence feeds and developments, as well as the infrastructure and vulnerability status of the organization. Also carried out in collaboration with other players in cybersecurity.

5.3.3 Incident Analysis and Response

This capability has six subheadings. These are,

1. Incident Analysis
2. Tradecraft Analysis
3. Incident Response Coordination
4. Countermeasure Implementation
5. On-site Incident Response
6. Remote Incident Response

- Incident Analysis

Extended, in-depth analysis of potential cyberattacks and advices from other participants of the SOC. This capability is usually performed within the SOC's incident escalation process by analysts in tiers 2 and above. In order to support an appropriate and effective response, it must be

completed in a specific time frame. Usually this skill includes analyzes using different data objects to evaluate who, when, when, where and why of an attack. And its extensions. How can loss be minimized and how to recover? An expert, usually with a suggestion for further action, may log the results of this review.

- Tradecraft Analysis

Carefully orchestrated adversary obligations by which SOC participants perform a suspended "down-in - the-weeds" review and analysis of adversary TTPs in an effort to better recognize and inform ongoing surveillance. Such operation is different from other techniques as, it sometimes requires the ad hoc instrumentation of networks and structures to concentrate on an item of concern, such as a honeypot, and a competitor will be permitted to continue his activity without being cut off entirely immediately. Trending and malware and implant detection are increasingly supporting this capability which, in effect, will support the creation of cyber intelligence.

- Incident Response Coordination

Consult with concerned stakeholders to collect additional information on an event, understand its meaning, and assess the impact of the task. Most specifically, this task involves planning efforts to respond and reporting events. This service does not directly involve countermeasures being implemented by the SOC.

- Countermeasure Implementation

Initial action to respond to an incident to prevent, block or cut off the presence or damage of the opponent. Applicable countermeasures provide logical or physical isolation of the systems involved, firewall blocks, black DNS holes, IP blocks, patch implementation and deactivation of the account.

- On-site Incident Response

This job is performed with system owners and sysadmins in partnership. Typically, this will allow SOC representatives who are already present at or moving to the constituent position to apply hands-on experience in harm assessments, remove modifications made by an opponent, and return networks to a known good condition.

- Remote Incident Response

Work with constituents to remotely recover from an incident. It includes the same work as the reaction to the on-site accident. SOC members, however, have relatively little hands-on experience in the acquisition or retrieval of objects. Remote assistance is usually done by telephone and email or remote server or administrative interfaces such as Secure Shell (SSH) in rarer cases.

5.3.4 Artifact Analysis

Artifact Analysis has three major factors. These are listed in the below.

1. Forensic Artifact Handling
2. Malware and Implant Analysis
3. Forensic Artifact Analysis

- Forensic Artifact Handling

Collection and preservation of forensic objects such as hard drives or removable media in connection with an event in a way that facilitates its use in legal proceedings. This may include managing media when recording the custody chain, maintaining secure storage, and promoting verifiable bit-by-bit copies of evidence, based on authority.

- Malware and Implant Analysis

Often recognized as malware reverse engineering or just "reversing." Extracting malware from network traffic or web photos such as bugs, trojans, routers, droppers, etc. then decoding it to evaluate the existence. Usually, SOC participants would search for initial direction, actions, and possibly informal identification to determine the extent of an interference and facilitate timely response. This can include either the analysis of static code through decompiled or the analysis of runtime / execution or both. The primary purpose of this capacity is to facilitate successful tracking and reaction. Although it utilizes some of the same methods as conventional "forensics," in order to support legal prosecution it is not usually conducted.

- Forensic Artifact Analysis

Observation of digital objects, media, network traffic, mobile devices, usually by maintaining a comprehensive timeline of events to define the full extent and ground truth of an incident.

This utilizes methods related to some aspects of malware analysis but follows a process that is more extensive and recorded.

5.3.5 SOC Tool Life-Cycle Support

SOC Tool Life-Cycle Support is an essential for the security prevention and detection. Every day new vulnerabilities are discovered by attackers. As a defender, SOC must be prepared for these new ways. Zimmerman (2014, p.21) noted, SOC Tool Life-Cycle Supports divides into six and these are listed in the below.

1. Border Protection Device O&M
2. SOC Infrastructure O&M
3. Sensor Tuning and Maintenance
4. Custom Signature Creation
5. Tool Engineering and Deployment
6. Tool Research and Development

- Border Protection Device Operation and Maintenance

Border protection tools (e.g. firewalls, network proxy, e-mail proxies, and internet filters) service and management. Requires system security changes and CMs, sometimes in response to a threat or accident. This operation co-ordinates directly with a SOC.

- SOC Infrastructure Operation and Maintenance

It involves SOC IT hardware such, computers, workstations, scanners, relational files, trouble-ticketing systems, networks with storage area (SANs) and tape backup. If the SOC has its own region, management of its routers, switches, firewalls, and domain controllers, if there is any, would possibly include this. O&M monitoring systems, operating systems and equipment may also be used.

- Sensor Tuning and Maintenance

Maintenance and feeding of SOC-owned and operated sensor platforms: IDS, IPS, SIEM, etc. It involves upgrading existing signature IDS / IPS and SIEM modules, optimizing their signature sets to hold the number of incidents at acceptable levels, mitigating false positives, and

retaining sensors and data feeds ' up / down health status. SOC members involved in this operation need to be keenly aware of the SOC's management requirements so that the SOC can keep pace with a constantly evolving world of continuity and hazard. Modifications to any in-line prevent systems (HIPS / NIPS) are planned with the NOC or other IT management regions. This functionality can require extensive ad hoc scripting to transfer data and combine software and data feeds.

- Custom Signature Creation

Authorizing and enforcing initial monitoring system identification information (IDS fingerprints, SIEM usage cases, etc.) based on current risks, vulnerabilities, policies, tasks, or other situation details. This ability optimizes tools at the fingertips of the SOC to fill holes left by the signatures provided commercially or by the organization. The SOC can discuss with other SOCs its specially designed signatures.

- Tool Engineering and Deployment

Market research, design development, designing, innovation, installation, implementation, and upgrade of SOC hardware, primarily based on Free or Open Source or Commercial Off - the-Shelf technologies. The service offers budgeting, buying and recapitalizing SOC programs on a regular basis. SOC must keep a close eye on a growing threat ecosystem, adding new technologies in a short period of time in keeping with the project's requirements.

- Tool Research and Development

R&D of design software where there is no sufficient technology for industrial or open source operations. The spectrum of this operation varies from the production of code for a recognized, standardized problem to more than a year academic research implemented to a more complicated task.

5.3.6 Audit and Insider Threat

This section examined in four subtitles. And these are listed in below.

1. Audit Data Collection and Distribution
2. Audit Content Creation and Management
3. Insider Threat Case Support
4. Insider Threat Case Investigation

- Audit Data Collection and Distribution

Gathering of a number of data feeds related to protection for purposes of identification and review of incidents. Such selection system can also be used to enable the delivery and eventual recovery of audit data outside the reach of the SOC task for on-demand investigation or analytical purposes. Such capacity requires long-term processing for use by components outside the SOC of security-relevant data.

- Audit Content Creation and Management

Creation and modification of SIEM or log management material to help audit analysis and identification of abuse by constituents. This service relies on the capacity of audit data transmission, supplying not only a raw data feed, but also content built for non-SOC constituents.

- Insider threat Case Support

Find tips for possible cases of insider attacks such as espionage, fraud and theft. The SOC must send off an event of concern to other investigating structures. The SOC will provide more supervision, evidence gathering and review on behalf of these investigating agencies in favor of an insider danger case.

- Insider Threat Case Investigation

The SOC takes advantage of its own autonomous administrative or legislative authority to investigate insider risks, including concentrated or extended surveillance of specific individuals, with the need for additional agency assistance or authorities. For fact, few SOCs have such authority outside the law enforcement community, and they typically operate under the control of another agency.

5.3.7 Scanning and Assessment

In this section includes four subtitles. These are listed and described in below.

1. Network Mapping
2. Vulnerability Scanning
3. Vulnerability Assessment
4. Penetration Testing

- Network Mapping

Consistent, periodic mapping of constituency networks across automated or manual methods to realize the constituency's volume, shape and circumference interfaces.

- Vulnerability Scanning

Consistency host checking about vulnerability status, generally focused on the modification of each device and enforcement with protection, primarily by automated, centralized resources. This leads the SOC to fully understand what it needs to protect, as with network analysis. The SOC can lend this data back in a study or overview form to community members. This task is conducted on a routine basis and is not part of a particular assessment or workout.

- Vulnerability Assessment

Total awareness, open-security evaluation of system, sometimes referred to as "Blue Teaming." SOC members work with sysadmins to analytically examine their system security architecture and vulnerabilities across scans, system settings update, documentation analysis of system development, and presentations. Such operation will use resources for network and vulnerability scanning, plus more aggressive technology used for inquiry schemes. Together with necessary remediation, tier members release a report of their results from this study. SOCs view risk analyses as an opportunity to expand the scope of surveillance and the awareness of the population of their analysts.

- Penetration Testing

Zero-knowledge or constrained-knowledge assessment of a given constituency region, also known as "Red Teaming." SOC participants perform a simulated assault on a constituency section to determine the vulnerability of the goal to an actual attack. Such activities are usually performed only with the approval and authority of the managers of the highest level within the continuity and without the owners of the program. Using tools can actually execute assaults through variety of means: buffer overflows, insertion of Structured Query Language (SQL), and input fuzzing. Generally, Red Teams would tailor their objectives and resources to mimic that of a single attacker, maybe simulating the operation of an enemy that could commence with a phishing attack. When the project is over, a report with its results will be generated by the team in the same way as a risk evaluation. Nevertheless, since penetration testing exercises have a limited set of objectives, they do not address as many areas of system configuration and

best practices as an evaluation of risk should. SOC employees will only manage Red-Teaming operations in some situations, with a selected third party doing most of the individual testing to ensure the participants have no previous knowledge of constituent processes or flaws.

5.3.8 Outreach

This section divides into six subtitles and these are listed in below.

1. Product Assessment
2. Security Consulting
3. Training and Awareness Building
4. Situational Awareness
5. Redistribution of TTPs
6. Media Relations

- Product Assessment

Checking the safety features of target items purchased by representatives of the electorate. Similar to one or a more hosts ' miniature risk tests, this method provides for a thorough analysis of the strengths and weaknesses of a particular product from a security perspective. This may contain monitoring products "in-house" rather than remote supply or pre-production services evaluation.

- Security Consulting

Providing technology guidance to non-CND constituents; implementing new systems integration, business continuity, and disaster recovery planning, safety strategy, safe programming guides and other initiatives.

- Training and Awareness Building

Proactive recruitment to residents to advocate general consumer awareness, updates, and other instructional resources to help them learn different safety problems. The key objectives are to help constituents defend themselves against common threats such as phishing schemes, more safe end networks, raise awareness of the services provided by the SOC, and help constituents monitor accidents correctly.

- Situational Awareness

Normal, routine repackaging and dissemination of the SOC's awareness of constituency properties, networks, risks, events, and constituent weaknesses. Such capacity extends beyond strategic intelligence delivery, improving the component's awareness of the constituency's cyber security environment and parts of it, promoting successful decision-making at all levels. Through some kind of SOC database, web service, or email delivery list, this information can be given automatically.

- Redistribution of TTPs

Sustained distribution of SOC internal items in a more organized, decorated, or standardized system with other users such as collaborator or subordinate SOCs. This can include almost anything that the SOC creates alone. Quid pro quo theory also applies, bidirectional knowledge exchange between SOCs.

- Media Relations

It is the SOC's duty to disclose information without impacting the constituency's credibility or continuing response operations.

5.4 SOC Architecture

There are many ways to build an SOC which fulfills a set of requirements. Each SOC will be special but there will be common elements for organization. But the architecture has two categories such as distributed or integrated (EPRI, 2013).

5.4.1 Multi-Center Distributed Architecture

A distributed multi-center architecture is based on a hierarchical SOC framework and is shown in Figure 5.5. Every business unit is responsible for handling alerts in real-time in this system and only important alarms are placed in charge of the SOC staff (EPRI, 2013).

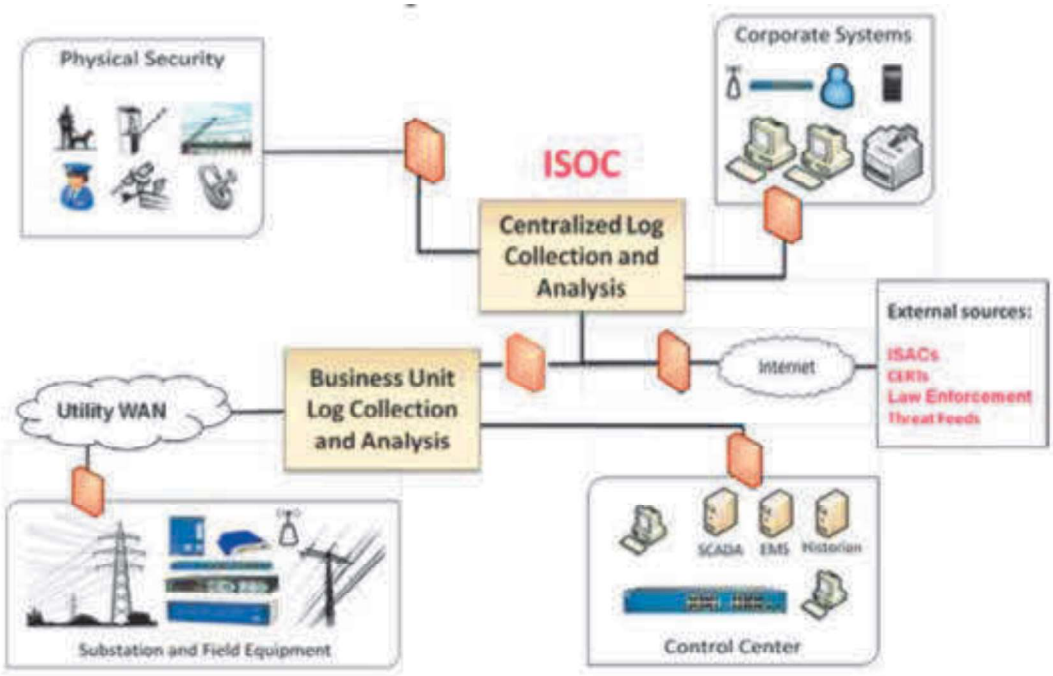

Figure 5.5 Multi-Center Distributed SOC (EPRI, 2013)

Advantages of Multi-Center Distributed SOC,

1. Reduces preparation costs for SOC workers, since they do not need to be specialists in all the areas of the service.
2. Minimum number of personnel needed by SOC.
3. Decreases the false positives for SOC workers, since they only collect vital warnings.

Disadvantages,

1. SOC workers have no real-time view across the organization, making it difficult to connect incidents and warnings that may seem uncritical to the domain personnel.
2. For each business unit, SOC personnel must create clear policies and procedures to define important warnings which should be brought to the attention of the SOC.

5.4.2 Fully Integrated Architecture

A fully integrated infrastructure provides real-time control for all utility business units, administrative processes, operational units and physical security. Major companies with significant resources will likely use this strategy when contributing to cyber security. Shown in Figure 5.6.

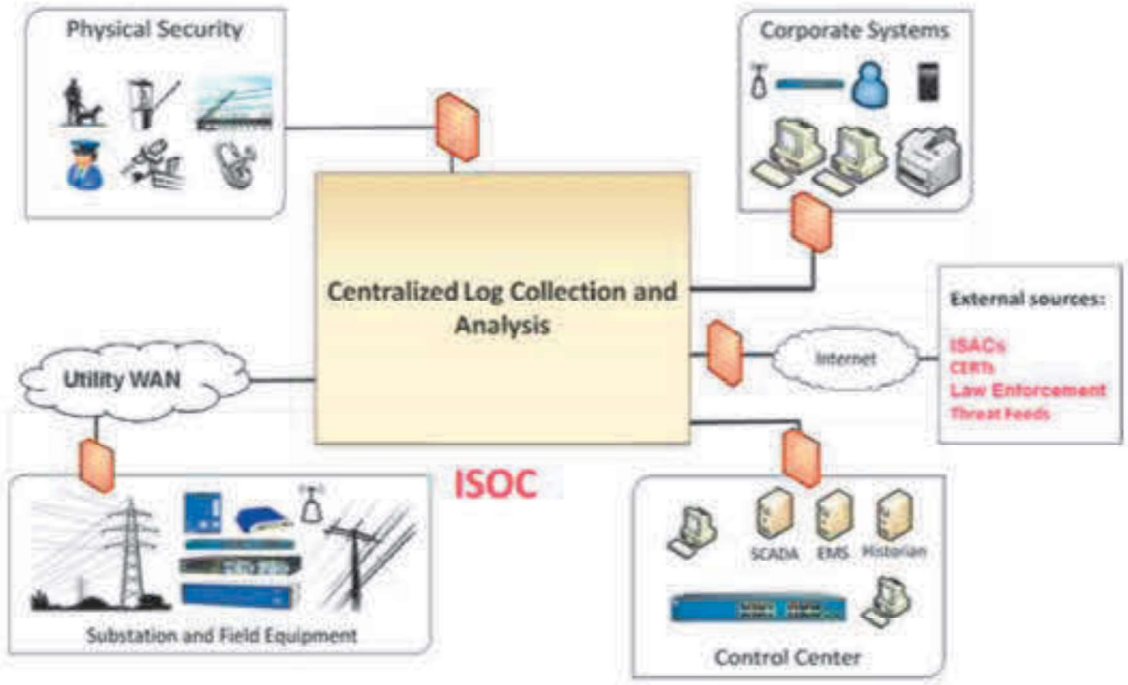

Figure 5.6 Fully Integrated Architecture (EPRI, 2013)

Advantages of Fully Integrated Architecture,

1. Brings real-time situational awareness throughout the business.
2. Better monitoring of incidents involving cross-business units, as SOC workers will connect activities across the organization.
3. Develops organizational resources to recognize and respond to events through multiple units of industry.
4. Promotes an intelligence-driven approach to identifying accidents.

Disadvantages of Fully Integrated Architecture,

1. Needs personnel to be experts in multiple units of the utility business.
2. Needs well-trained staff to provide information security capabilities and support forensics to the various business systems.

5.5 Types of SOC

The type of SOC is decided by requirements and needs of an organization. There are three types of SOC. The major concern of the architecture is the use of third-party security service providers to handle the SOC. MSSPs (Managed Security Service Provider) provide the software for

tracking and controlling intrusion detection systems and firewalls. Other security functions like patch management and security audits may also be supported by MSSPs. A company can reduce its own security staff by outsourcing these services and focus on its core business. At present, multiple companies rely on MSSPs to provide insight and assistance to their corporate security operations centers (EPRI, 2013).

1. Externally Managed SOC
2. Internally Managed SOC
3. Hybrid Managed SOC

5.5.1 Externally Managed SOC

This method extends the centrally controlled ISOC to include operating device logs as well as physical security.

Reduces criteria for SOC staff of the company for skills and training. Takes advantage of large global presence MSSPs, allowing them to identify new threats and attack signatures early. Reduces ISOC operating costs. This type of SOC provides the utility with access to a' kit' of resources, including centralized perimeter control. These are the benefits of externally managed SOC (EPRI, 2013).

On the other hand, disadvantages are, most MSSPs have no power-system expertise. A MSSP may not be able to meet utility-specific data processing criteria from critical systems. Utilities lack input and leverage over the accident identification process, making it difficult to change the procedure and minimize false positives (EPRI, 2013).

5.5.2 Internally Managed SOC

In this type, the utility has inculcated both parts of its ISOC management and staffing.

Some benefits are, provides full control over the event identification and reaction procedures by the service. Cuts down the concerns about the security logs and sensitive data being stored and transported. Develops the utility's powerful internal cyber incident response capabilities (EPRI, 2013).

Some disadvantages are, needs the company to maintain operations 24x7. Requires that utility personnel be trained in multiple safety disciplines. Needs utility staff to monitor new information about risks and may demand that they receive clearances from government security. Needs the ISOC security tools to be completely managed by the service staff and continuously adjusted by the utility to minimize false positives and false negatives (EPRI, 2013).

5.5.3 Hybrid Management SOC

A hybrid management strategy attempts to merge the two previous strategies to suit the utility's skills and finances.

Advantages are, decreases the SOC criteria for personnel. Takes advantage of MSSP's monitoring experience and skills in vulnerability detection. Develops the utility's own event response capability (EPRI, 2013).

Disadvantages are, the organization loses control of a part of the process of crisis response. This includes transfer of knowledge in both directions: knowledge of the power systems from utility to MSSP and knowledge of protection from MSSP to utility (EPRI, 2013).

5.6 Maturity Models and SOC Maturity

5.6.1 Maturity Models

As mentioned in the previous chapters, SOC can be useful internally or externally. And noticed above both type have advantages and disadvantages. According to Jacobs, “there are no objective mechanisms to determine the maturity level of the processes and service offerings within the SOCs. Also, geographically dispersed SOC’s from the same organization can differ in maturity and capability, and there is currently no objective means to measure the disparity.” (Jacobs P., et al, 2013).

If defining a SOC's maturity level, that would be cautious to use existing IT management framework, such as Control Objectives for Information Technology (CoBIT) and Information Technology Information Library (ITIL), associated with ISO / IEC 27001 information security

frameworks. The CoBIT framework provides an overview of IT at work and is aided by ITIL, which covers operational usefulness and efficiency (Jacobs P., et al, 2013).

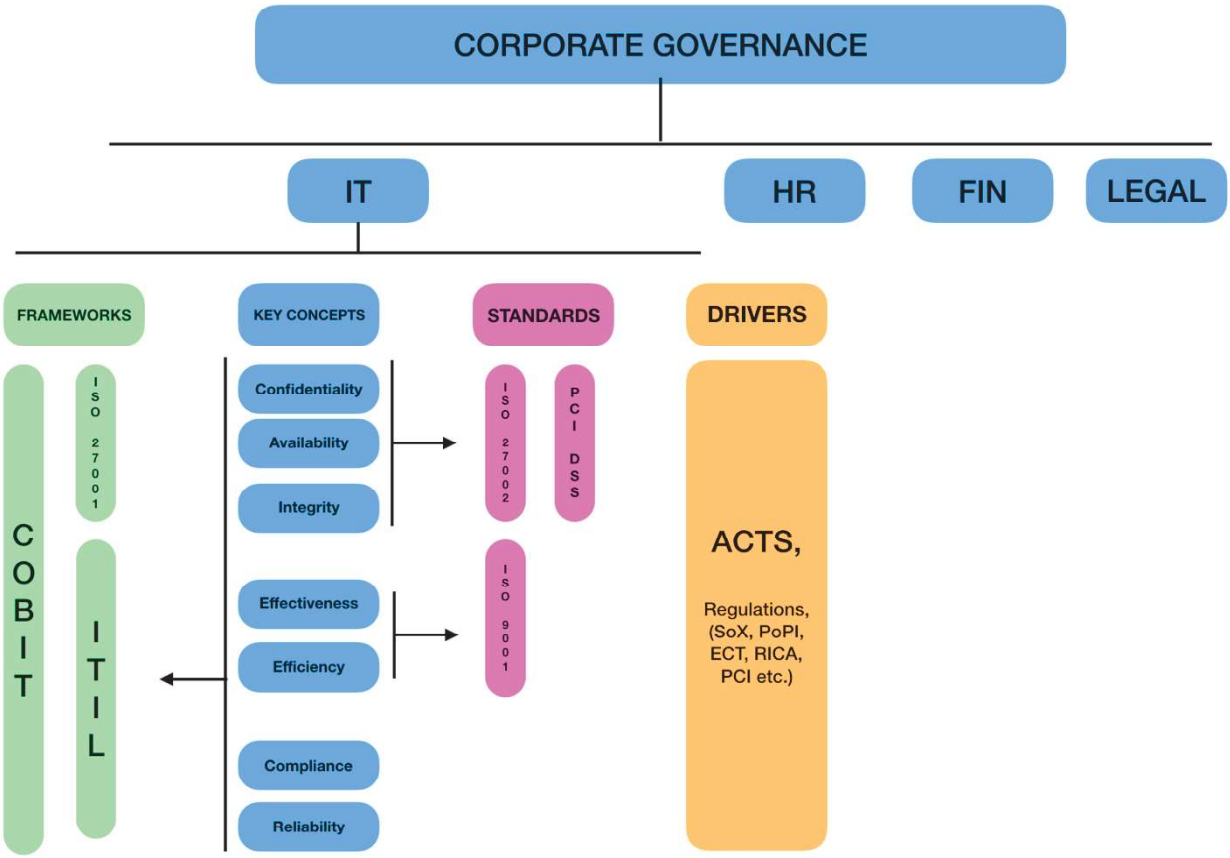

Figure 5.7 “Relationship between Standards, Frameworks and their drivers” (Jacobs P., et al, 2013)

In furtherance of create a sustainable model, SOC’s must provide each aspect, capability and the successful rate of functionality delivering, maturity (Jacobs P., et al, 2013).

According to SEI (Adler M, et al, 2007), CoBIT has five maturity levels to increase management and IT progress. And these five levels are,

- 0 Non-Existent
- 1 Initial / Ad Hoc

- 2 Repeatable but Intuitive
- 3 Defined Process
- 4 Management and Measurable
- 5 Optimized

These mentioned maturity models can be used for helping to create a profile because they do not have hundred percent success rate.

The ITIL Process Maturity Framework (PMF) also identifies five Process Maturity Levels. ITIL focus more on the Operational aspects of the IT Key concepts, and this is reflected in the fact that their framework addresses Process Maturity (Jacobs P., et al, 2013).

According to Jacobs the five ITIL Process Maturity Framework levels,

- 1 Initial
- 2 Repeatable
- 3 Defined
- 4 Managed
- 5 Optimized

According to Wim Van Grembergen et al, "*The control objectives of COBIT indicate for the different IT processes what has to be accomplished, whereas other standards, such as ITIL, describe in detail how specific IT processes can be organized and managed.*" (Grembergen W. V., et al, 2005).

The Capability Maturity Model (CMM) additionally has five maturity level models. And CMM concentrate on business software process and the assessment of the capability of these processes (Curtis B., et al).

NIST noted five security maturity levels. These are,

- Level 1 Policies
- Level 2 Procedures
- Level 3 Implementation
- Level 4 Test
- Level 5 Integration

Jacobs P. noted that, The International Systems Security Engineering Association (ISSEA) created a Capability Maturity Model (CMM) and named as Systems Security Engineering Capability Maturity Model (SSE-CMM). These levels are,

- Level 1 – Base practices are performed informally
- Level 2 – Base practices are planned and tracked
- Level 3 - Base practices are well defined
- Level 4 - Base practices are quantitatively controlled
- Level 5 - Base practices are continuously improving

According to Akridge and Chapin, methodical approach for assessing the sophistication of a technological or administrative security check should be produce repeatable and acceptable measurements of organizational or client safety posture and service, measure anything which applies value to the customer or association, decide advances in security posture and customer service delivery. Help to determine the way in which security checks and resources to implement the security program should be applied (Akridge & Chapin, 2005).

5.6.2 SOC Maturity

Jacobs P., et al, has noted that six stage of maturity model at SOC based on industrial maturity models. The cube in Figure 5.8 should support the weight and amount of SOCs to be assigned. We recommend a hardly higher weighting for complexity owing to the value of operation consistency. System complexity is weighted higher than capacity, because it is more important than the number of skills to sustain, conduct, and repeat (Jacobs P., et al, 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 Measureable (CoBIT) and Continuous Improvement (CITI-ISEM)
5	Continuously Optimised	Optimised (CoBIT), Continuously Improving (CITI-ISEM), Continuously Improving (SSE-CMM)

Table 1 “Process Maturity” (Jacobs P., et al, 2013).

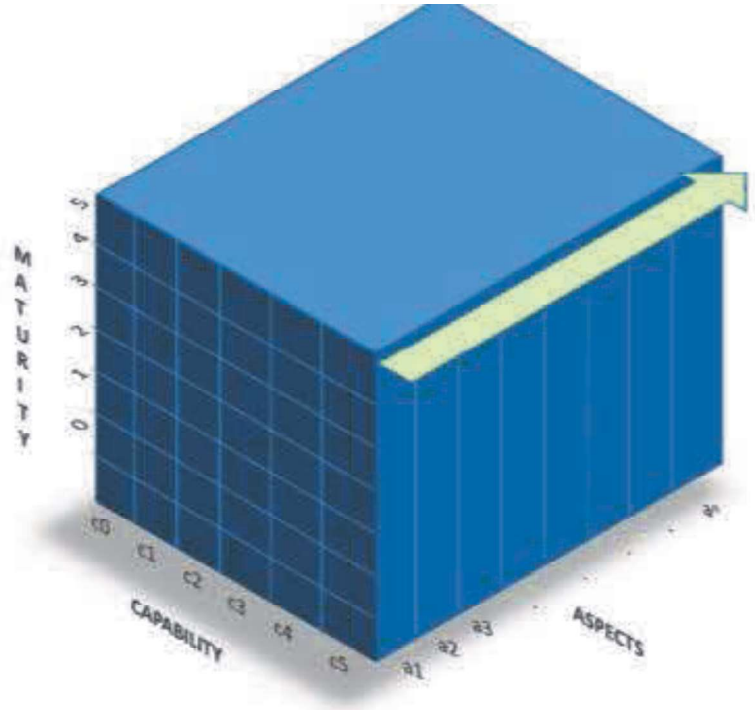

Figure 5.8 "SOC Classification Cube" (Jacobs P., et al, 2013).

Jacobs P., et al developed a formula of calculation of SOC Score. And the formula is defined as,

$$S = \frac{\sum_1^n (\alpha C_i + \beta M_i)}{0.05\ X\ n}$$

"SOC Score = Sum of all applicable aspect scores, where each aspect is scored on Capability and Maturity expressed as a score out of 100." (Jacobs P., et al, 2013).

Jacobs noted that, *"This will provide a weighting which can be referenced against the provided map. SOC Managers and customers should strive for a high maturity and high capability level. Based on the business requirements, it would also be possible to weigh specific aspects higher than others."* (Jacobs P., et al, 2013).

Jacobs claimed that "*We have used the above approach and applied it to rate a known SOC provider in South Africa, which we are well acquainted with. The breakdown of the individual aspects as shown in Figure 5.9, and the total score of the SOC is 46.4 shown in Table 2. While*

this particular SOC service has some strong services, the majority of the services are below par, and this is reflected in the overall score. As discussed in Section IV, we intend to extend this rating formally across multiple providers in South Africa, which would allow us to build a comprehensive analysis of the SOC services market in South Africa, including the strengths and weaknesses of various players together with the overall industry norms." (Jacobs P., et al, 2013).

Figure 5.9 Rating of SOC (Jacobs P., et al, 2013).

	Aspect	Maturity	Rating
REPORTING	2	2	2
LOG COLLECTION	3.5	3	3.2
LOG RETENTION	2	2	2
LOG ANALYSIS	2	1	1.4
MONITORING	2.5	2	2.2
CORRELATION	3	3	3
DEVICE TYPES	3	4	3.6
INCIDENT MGMT	2	4	3.2
REACTION TO THREATS	1	2	1.6
THREAT IDENTIFICATION	1	1	1
	22		23.2
	2.2		46.4

Table 2 South Africa MSSP Rating (Jacobs P., et al, 2013).

CHAPTER 6

DISCUSSION

The expansion of monitoring services needs better log analysis work. Because some monitoring tools may not perform at expected success level. For this reason, Artificial Intelligence (AI) comes up to the surface to improve and aid to IDS/IPS tools. AI aims to reduce the workload in logging and monitoring in real-time analysis. In addition, to improve of the judgement accuracy is another goal of the AI in SOC. AI is capable of assisting to Tier 1 and Tier 2 events. This, can be a beneficial to Tier 1 and Tier 2 personnel, is an advantage. In Figure 7.10 shows that it is about 50% of the analysis logs compared to former status before using AI have been reduced successfully, thereby leading to improvements in the operational efficiency of the analysts. However, when the setting threshold value is adjusted to substantially increase the accuracy of the false positive detection as "false-positive," false-negative rarely exists as a trading-off. Since it is crucial to hold false negatives as similar as null considering the properties of this service, the threshold setting is tuned very carefully to avoid false negatives.

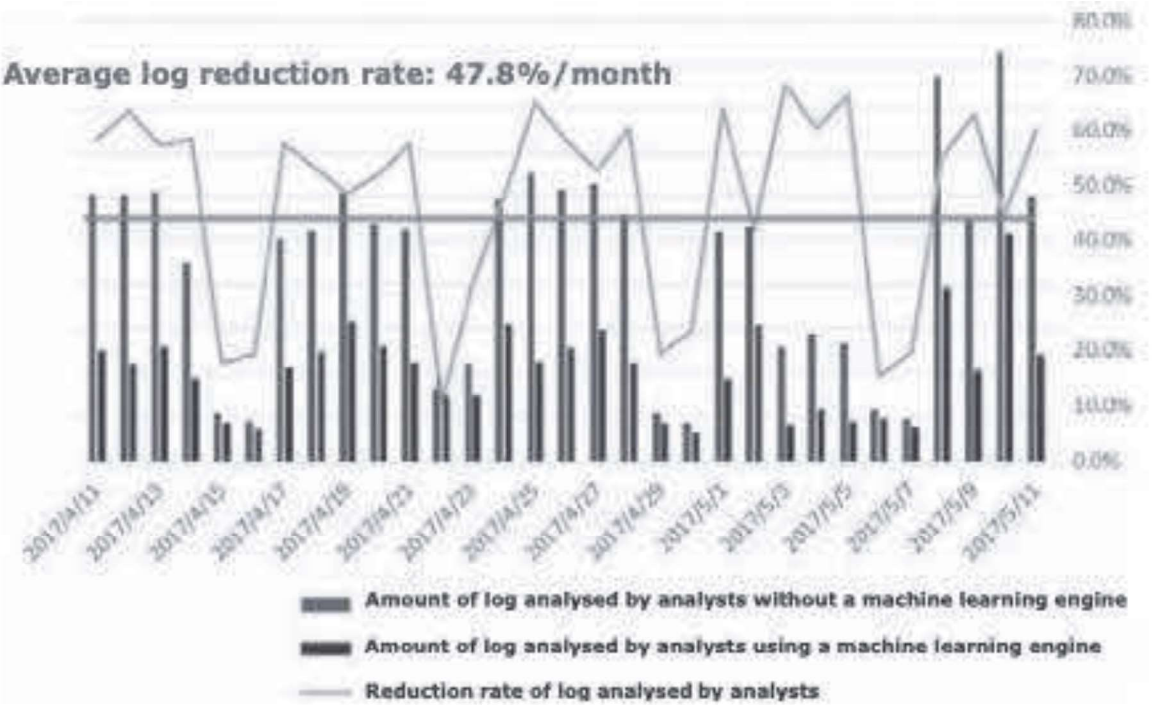

Figure 7.10 Log Analysis Efficiency Improvement Using AI (NEC, 2018).

By using AI for self-analysis and minor decisions. Events that occupy a large part of analysts' operations can focus on more important activities of this kind. As a study of methods to respond to advance attacks and improve their detection accuracy. According to Arimatsu, Yano and Takahashi (NEC, 2018), positive use of AI can promote standardization of the quality of monitoring services and encourage innovative efforts of the analysts. The logs and warnings of a single safety system are frequently inadequate for an observer to determine the extent of the incident, requiring more time for review. There will also be the same instances as alert succeeds in detecting a real threat but is unable to detect it. Determining whether or not it was successful when the events are considered to be Level 3. This is one disadvantage of using AI. Because such cases mean an issue from the viewpoint of analysis accuracy. Once logs and warnings from various devices (inputs) and assessment reports from analysts (outputs) are collected as data, advanced learning data that can show high correlations between inputs and outputs are required to be compiled. It is also estimated that the accuracy of the AI analysis can also be improved and the scope of use of AI in the SOC expanded further.

Establishing a SOC in a cloud environment is a new approach to provide cloud services with information security and event management. However, the recommendations made did not specify a specific model for SOC implementation in a cloud computing environment. Probst et al. (An Approach for Security Evaluation and Analysis in Cloud Computing, 2013) proposed an automated review of and assessment of cloud protection mechanisms effectiveness. The emphasis was on testing access control and intrusion detection systems, which is only part of the process. The overall process of cloud risk management and assessment. Furthermore, their approach is confined to the cloud infrastructure computing. Cloud service providers are assumed to allow the SOC provider to deploy SOC agents in their security devices for system event collection purposes. Also, cloud service providers are assumed to allow the SOC system to respond to an event that may require a change in a security device. Providers benefit from an increase in public trust, quality of service, and adoption of cloud services. This is achieved by allowing customers to employ SOC to oversee their host cloud services and provide security assurance in real time.

A trusted third party may operate the SOC system to manage the security of cloud providers Devices and Equipment. The trusted SOC party will have the best practices in operating and supporting various platforms for security operation centers. That provides the security and transparency that cloud customers require. Delegating a third party to monitor and manage security systems for the cloud provider encourages cloud providers to increase investment in functionality and security of service. The SOC entity operating as a business interest will invest in well-trained security personnel and will adopt operational and analytical procedures established by SOC. These procedures will align with the business requirements of the cloud providers and customers. It should also establish an organizational relationship with cloud service providers and customers and have regular meetings. This facilitates productive discussions and the sharing of information that can help to update service level agreements and regulatory compliance requirements. It can also support the development and vulnerability assessment of customer software.

Hybrid SOC architecture provides for many midmarket organizations and some large companies, the operation of a SIEM seems overwhelming given the need for SIEM administration staff expertise, threat research, and security intelligence analysis. To maximize effective operational coverage the SIEM environment must be continuously monitored, managed, tuned and extended. The solution can be set up quickly with the hybrid approach, has the flexibility to scale efficiently, and minimizes risks and unforeseen costs. The service provider offers extended resources for the operation of the SIEM environment to supplement your internal staff. The organization now has access to the named resources with a hybrid solution to overcome the staffing challenges. Imagine an arrangement in which the MSSP and Tier 3 internally handled tickets for Tier 1 and Tier 2 security events. The service provider would provide wide-ranging insights derived from their global reach through hundreds and thousands of consumer settings, thus improving the operation 's threat awareness. Imagine having access to global intelligence threats and highly skilled intelligence security analysts as a normal extension of your internal resources. The excellent thing with hybrid SOC architecture is that companies of all sizes will benefit from the proven benefits of a full SIEM for security operations.

CHAPTER 7

CONCLUSION

As mentioned in the above chapters, SOC will be the major security concept in the future days. As a consequence of this, managing and building a SOC gains so much importance. This thesis aimed two key points. The first one is to become a roadmap for building a SOC. And the second point is to examine and supervise the maturity scores of the other SOC's in the world and making improvements.

Sans Institute noted that "cyber security incidents will cause significant financial and reputation impacts on enterprise. In order to detect malicious activities, the SIEM (Security Information and Event Management) systems is built in companies or government. The system correlates event logs from endpoint, firewalls, IDS/IPS (Intrusion Detection/Prevention System), DLP (Data Loss Protection), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), Windows/Unix security events, VPN logs etc." (SANS Institute, 2013).

In the above citation shows the importance of SOC. And this thesis tried to accomplish to find the new solution out to the cybersecurity area. As a conclusion, this thesis came up to be as an authority in cybersecurity domain. In the conclusion, SOC objectives and aims can be listed as,

- 7x24x365 monitoring against cyber incidents
- Real-time analysis and response
- Forensic analysis
- Penetration testing
- Ensuring continuity on web domain
- To prevent against intrusion
- To search and provide some certifications for employees from institution such EC Council, CISCO and SANS
- Experienced and qualified stuff

After all, SOC must keep maturity score high, while having these. And making good communication between the stuff and the companies. To sum up, these are the reasons for making the SOC an authority in the cyberspace domain.

The below topics have been considered as important for the future researches:

- To make own software tools
- To develop more secure ways of communication
- To make own certificate programs
- To build and improve communication between international cyber intelligence units.

In the future, the SOC will be able to integrate a service that can track several log data, including servers and clients, and then the SOC will receive more logs and warnings than it does today. In order to make this possible, it is necessary to make good use of the Artificial Intelligence (AI) to enhance the role of filtering events of low significance and to prepare a mechanism that allows analysts to evaluate and make decisions only on important events.

REFERENCES

Aggarwal, Palvi & Grover, Antra & Singh, Saumya & Maqbool, Zahid & Pammi, V. S. Chandrasekhar & Dutt, Varun. (2015). Cyber Security: A game-theoretic analysis of defender and attacker strategies in defacing-website games. 10.1109/CyberSA.2015.7166127.

Alruwaili, F. F., & Gulliver, T. A. (2014). SOCaaS: Security Operations Center as a Service for Cloud Computing Environments. *International Journal of Cloud Computing and Services Science*, *3*(2089-3337), 87–96. Retrieved from http://iaesjournal.com/online/index.php/ IJ-CLOSER

Akridge S. and Chapin D. A., How Can Security Be Measured? *Information Systems Audit and Control Association.*, 2005. [Online]. Available: http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Pages/How-Can-Security-Be-Measured.aspx.

Bidou R. (2005). Security Operation Center Concepts & Implementation.

Bill Curtis et al, Software Capability Maturity Model (CMM). [Online]. Available: http://www.itgovernance.co.uk/capability-maturity- model.aspx.

Cisco Systems, How to Build Security Operations Center (SOC), 2007. [Online]. Available: ftp://ftp-eng.cisco.com/cons/workshops/SP-Powersession-Thailand-Jan-2007/SPSEC-610-Security-Operations- Centers-Basics-V ersion-2.pdf.

Cyber Security Introduction – javatpoint [Online]. (n.d.). Retrieved from https://www.javatpoint.com/cyber-security-introduction.

Dempsey, K., Dempsey, K., Chawla, N., Johnson, L., Johnston, R., Jones, A., Orebaugh, A., Scholl, M. and Stine, K. (n.d.). *Information Security Continuous Monitoring (ISCM) for federal information systems and organizations*.

EY, Security Operations Centres against Cybercrime, Top 10 Considerations for Success, 2013.

IBM, Strategy Considerations for Building a Security operations Centre, 2013.

IT Governance, Software Capability Maturity Model (CMM). [Online]. Available: http://www.itgovernance.co.uk/capability-maturity- model.aspx.

Kowtha, S.; Nolan, L.A.; Daley, R.A., Cyber security operations center characterization model and analysis, Homeland Security (HST), 2012 IEEE Conference on Technologies for, vol., no., pp.470,475, 13-15 Nov. 2012.

Mark Adler et al, CobiT 4.1 Framework, 2007. [Online]. Available: http://www.isaca.org/Knowledge- Center/cobit/Documents/CobiT_4.1.pdf.

McAfee White Paper, Creating and Maintaining a SOC, the Details behind Successful Security Operations Centres, 2011.

Melnick, J., Matthews, K., Matthews, K., Melnick, J., Brooks, R., Brooks, R., & Melnick, J. (2018, May 15). Top 10 Most Common Types of Cyber Attacks. Retrieved from https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/.
NEC Technical Journal Vol.12 No.2, Special Issue on Cybersecurity

NIST, Security Maturity Levels, 2012. [Online]. Available: http://csrc.nist.gov/groups/SMA/prisma/security_matu rity_levels.html.

P. Jacobs, A. Arnab and B. Irwin, Classification of Security Operation Centers, *2013 Information Security for South Africa*, Johannesburg, 2013, pp. 1-7. doi: 10.1109/ISSA.2013.6641054

RSA Technical Brief, Building an Intelligence-driven Security Operations Centre, 2013.

SANS Institute. (2013). The 6 Categories of Critical Log Information. https://www.sans.edu: Retrieved from https://www.sans.edu/cyber- research/security-laboratory/article/6toplogs

S. Schinagl, K. Schoon, and R. Paans, "A Framework for Designing a Security Operations Centre (SOC)," *2015 48th Hawaii International Conference on System Sciences*, 2015.

T. Probst, E. Alata, M. Kaaniche, V. Nicomette, & Y. Deswarte, "An Approach for Security Evaluation and Analysis in Cloud Computing," Safecomp, France, September 2013.

Types of Cyber Attacks - javatpoint. [Online] (n.d.). Retrieved from https://www.javatpoint.com/types-of-cyber-attacks.

Van Grembergen, Wim & De Haes, Steven. (2005). Measuring and improving IT governance through the balanced scorecard. Information Systems Control Journal. 2. 35-42.

Zimmerman, C., Ten Strategies of Word-class Cybersecurity Operations Center, Mitre Corporation, 2014.