Chapter 1

INTRODUCTION

The last two decades can fairly be called the age of advancement in cyber space and data networking technology such as the internet and intranet. From household gadgets to professional services, every aspect of life has experienced an increased dependency on data and resultantly information technology has assumed utmost importance, even in day to day operations of organizations and individuals. Organizations and enterprises, in particular, have resorted to either deploying dedicated information technology (IT) architectures for storing, sharing and accessing their data or outsourcing the same to other professional companies who provide the information technology services on charges.

Organizations can be broadly subdivided into two categories, commercial and private. Commercial organizations can have their own basic IT architectures or they can outsource the same to other professional firms who provide them various data handling facilities as services on payment. Whereas private organizations which are sensitive in nature such as Government, Military and other secure enterprises cannot afford to outsource any of their service and need to raise their propriety infrastructure to handle their data for the obvious requirement of utmost confidentiality.

With such a huge advancement in and dependency on data handling IT infrastructures, comes the inevitable requirement of securing data. Organizations have endeavored to employ state of the art IT security equipment in order to protect their most critical asset, their data, from any possible breach or illegal access. However last two decades have also experienced an exponential increase in IT hacking, data breaches and cyber threats. Commercial and professional organizations, who have utilized top of the line cyber security measures, are still being affected by such threats. One logical reason for this fact is that although the organizations have installed adequate measures of IT security, most of these measures work in Silos [1]. Each individual security measure works separately to provide security in a disjointed fashion. This gives rise to the need of a mechanism which can monitor all security and operational equipment, in IT architecture, for security related events [1] and presents the owners with a holistic picture

of their organization's security posture. Security Operations Centre (SOC) is one such mechanism which can perform this task.

The concept of SOC has recently gained much popularity amongst enterprises, both commercial as well as private. Organizations have strived to establish their SOCs basing on the frameworks available in the market. These frameworks have been designed keeping in mind the requirements of commercial organizations which are very different and diverse in nature when compared to private, sensitive organizations, who tend to own their propriety IT infrastructure, hence called closed IT organizations in this thesis. When the same commercial SOC frameworks are implemented in closed IT organizations, they are found to be inadequate in the sense that they do not succeed in achieving the desired results, consequently making the SOCs of these organizations as ineffective entities. Alternatively there are no SOC frameworks available in the market that have been designed or tailor made keeping in mind the requirements and threat canvas of private, sensitive closed IT organizations [2].

This chapter will present the basic concepts relating to SOC as well as a brief overview of the problem which has been addressed in this thesis.

1.1 The Seriousness of Cyber Threat to Organizations

The advancement in IT infrastructures around the globe and the increased dependency of organizations on data has also given exponential rise to the compromises and breaching methodologies of such data. Over the past two decades, the canvas of cyber attacks has formidably transformed from a few simple off the shelf scripts to a threat which is real, much more technical, advanced and persistent. This threat has not only affected the commercial sector, which is heavily dependent on data automation, but it has also gravely endangered the sensitive organizations of our society, such as the government and Defence organizations, and critical infrastructure enterprises.

The under mentioned statistics that have been obtained from HACKMAGEDDON, a famous forum which analyses the cyber threat scenario around the globe, a fair idea of the seriousness of this threat can be obtained.

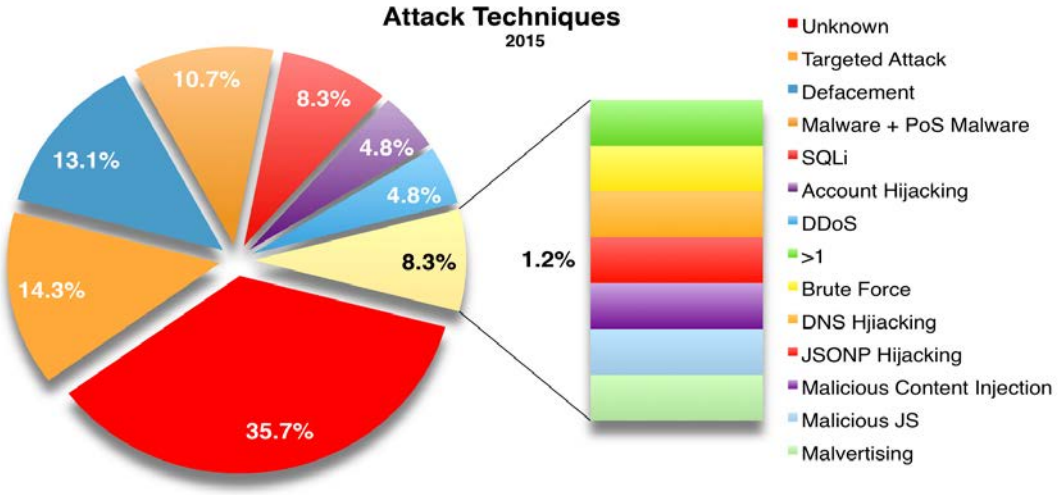

Fig.1: Year 2015, Percentage of different kinds of attacks carried out[3]

It can be noted that a large chunk of the subject attack techniques belong to the category of unknown, that is these are the attacks which have not been witnessed previously and against whom no mitigation or detection methods have been devised yet. In other words they are zero day attacks.

1.2 The Quantum of Threat to Sensitive Organizations

The phenomenon of cyber threats, hacking and data breaches has affected private and sensitive organizations as gravely as their commercial counterparts. The following figure provided by HACKAMGEDDON gives an overview of the sectors of society that have been victimized by cyber threats in year 2015.

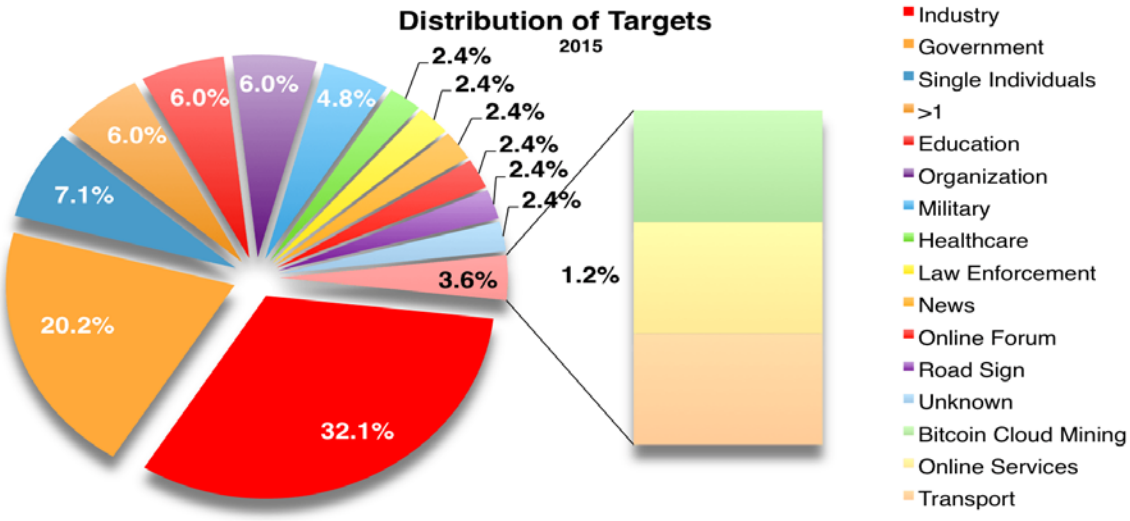

Fig.2: Targets of Cyber Attacks in Year 2015[3]

According to the above mentioned figure a sizeable portion of the targets, belongs to government, military and other sensitive private organizations. Another statistic obtained from ISACA confirms this state of affairs

Figure 1—Industry Representation

	FREQUENCY	PERCENT	VALID PERCENT	CUMULATIVE PERCENT
Advertising/marketing/media	7	0.6	0.6	0.6
Aerospace	12	1.0	1.0	1.6
Education/student	46	3.8	4.0	5.6
Financial/banking	260	21.3	22.4	28.0
Government/military—National/ state/local	162	13.3	14.0	41.9
Health care/medical	30	2.5	2.6	44.5
Insurance	42	3.4	3.6	48.1
Legal/law/real estate	5	0.4	0.4	48.6
Manufacturing/engineering	68	5.6	5.9	54.4
Mining/construction/ petroleum/agriculture	22	1.8	1.9	56.3
Pharmaceutical	9	0.7	0.8	57.1
Public accounting	17	1.4	1.5	58.6
Retail/wholesale/distribution	26	2.1	2.2	60.8
Technology services/consulting	357	29.3	30.7	91.6
Telecommunications/ communications	57	4.7	4.9	96.5
Transportation	18	1.5	1.6	98.0
Utilities	23	1.9	2.0	100.0
Total	1161	95.2	100.0	
Missing	59	4.8		
Total	1220	100.0		

Fig.3: Sectors of Industry affected by Cyber Attacks in 2015 [4]

According to the above quoted statistics, the second largest sector of industry that has been affected by cyber attacks belongs to government, military and other sensitive private enterprises. This confirms the fact that the threat to these organizations, termed as closed IT organizations in this thesis, is as formidable and real as it is to the commercial firms.

1.3 Introduction to the Concept of SOC

The concept of a Security Operations Center (SOC) is not relatively new to the IT community and dates back to almost two decades, but it is fairly recently that it has gained momentum and come into the limelight, owing to the exponential advancement in Cyber threat canvas. Since the business processes of various organizations developed an increased

dependency on their data and its associated IT infrastructure, this gave rise to the need to secure this data from unauthorized access and pilferage. Therefore organizations started employing numerous state of the art security mechanisms, such as IDS, IPS, firewalls, Antivirus, DLP e.t.c. These mechanisms were installed at all layers of the OSI model, to protect the organizations from possible data breaches and compromises. However, even employing so many security devices within the IT infrastructure proved to be inadequate when it came to stopping cyber attacks. The sole reason for this was that although the installed security devices were very efficient in themselves but they worked in isolation creating the phenomenon of security silos. Each device tried to mitigate the threat on its own level. There was no single, unified mechanism available to the organizations which could gather intelligence from all their security and operational devices and present them with a holistic picture of their security posture on one screen. This gave birth to the concept of Security Operations Centre (SOC). A SOC is a mechanism which gathers intelligence feed (in the form of events and flows) from all security and operational devices, employed within an IT architecture, and compares them against a pre defined set of rules to decide what all IT offences and violations have taken place within the organization. Furthermore it presents these offences to the security administrators in a holistic and consolidated manner on one screen [1]. Apart from this basic functionality, a SOC also contains the capability to respond to the emerging threats and carry out their detailed forensics as well as keep a check on the organization for compliance of security rules.

1.4 Definition of Closed IT Organizations

IT organizations can be divided into two broad categories, Commercial and Private. Those private organizations which are sensitive in nature, such as the Government, Military or Critical Infrastructure Organizations have far more stringent requirements of confidentiality as compared to their commercial counterparts. This necessity of maintaining utmost secrecy usually requires such sensitive organizations to lay out their own, propriety IT infrastructure. From end user equipment to the intermediate media, from data centre facility to server side applications, sensitive organizations establish their own infrastructure instead of outsourcing their requirements to commercial providers. Moreover most of these organizations have their own network i.e. intranet and do not use public connectivity of internet. Thus their IT infrastructure is closed in nature. Hence the term “Closed IT Organizations” has been coined to refer to such organizations in this thesis.

1.5 The Problem Encountered

When it comes to establishing and maintaining a SOC in Closed IT Organizations, a specific problem is encountered. The frameworks available in the market for establishing and maintaining SOC are designed for commercial organizations. When these frameworks are applied to closed IT organizations, they prove to be inadequate and lacking in their adaptability since these organizations are different in their nature, requirements, architecture and threat canvas owing to the closed nature of their infrastructure. No such framework is available in the market till date, which is designed specifically for closed IT organizations, keeping in mind the nature of their particular architecture, threat scenario and risk scope. This thesis carries out a research on developing a framework that can be utilized universally across such organizations for establishing and maintaining SOC.

1.6 Thesis Goals

The research conducted during this thesis, its outcome and analysis has been carried out keeping in mind the following goals:

- Propose an organizational structure of SOC for Closed IT Organizations.
- Propose a framework/ sequential methodology for establishment of SOC in these organizations.
- Devise standard criteria for selection of SIEM tools.
- Propose a basic set of intelligence required to be obtained from SOC in Closed IT Organizations (use cases).
- Propose a human resource structure required to run and maintain SOC in such organizations.

1.7 The Layout of Thesis

Apart from the introduction this thesis comprises of eight chapters. Chapter 2 elaborates the concept of Closed IT Organizations in further detail, highlighting the common architectures in vogue in such organizations as well as the significant differences that exist between the IT setups of these organizations and their commercial counterparts. Chapter 3 discusses, in depth, the concept of SOC, its common designs being followed around the globe and its functional units. Chapter 4 provides an overview of the literature review conducted in relation to this research and gives a gist of what all work has been carried out on SOC by previous researchers. Chapter 5 explains the problem statement. Chapter 6 describes the research and evaluation methodology that has been adopted during the course of the thesis. Chapter 7 describes the proposed framework in detail that has been formulated as an outcome of the research and

analysis carried out for the subject compilation. Chapter 8 evaluates the proposed framework against a set of key performance indicators (KPIs)/ metrics that were already decided upon in chapter 6. Furthermore it carries out a final analysis of the subject framework on industry accepted standards. Chapter 9 provides a way forward for the future work that could be taken on by other researchers, in order to take the presented concept further.

Chapter 2

THE CONCEPT OF CLOSED IT ORGANIZATIONS

There can be two main reasons why organizations establish their IT infrastructure. First, to pursue their commercial business goals, second to support private data processing necessary for their organizational objectives. This logically categorizes IT organizations into two types, the commercial enterprises and private organizations. Private organizations could be further divided into normal enterprises such as companies with local networking and data processing facilities (established for non commercial reasons), and sensitive IT establishments such as pertaining to Government, Military and other critical infrastructure organizations.

2.1 The Concept

The IT architectures of private sensitive organizations such as Government or Military are fundamentally different in their design and objectives as compared to their commercial or normal private counter parts. These organizations have a stringent requirement of keeping their data confidential and secure. This necessity of maintaining utmost secrecy usually compels such sensitive organizations to lay out their own, propriety IT infrastructure. Right from the end user equipment to the server farms in Data Centre, and all intermediate equipment, network and media, sensitive organizations tend to establish their own infrastructure. The phenomenon of outsourcing, any of these services to commercial providers, is highly discouraged due to the obvious reasons of security. Moreover most of these organizations maintain a private network i.e. intranet and do not use public connectivity of internet. Thus their IT infrastructure, whose prime focus is on being confidential, is closed in nature. Hence the term “Closed IT Organizations” has been coined to refer to such organizations in this thesis.

Since the objectives of design and service provision in closed IT organizations are different, therefore their threat canvas and risk scope also differs in its nature than the commercial enterprises. In such organizations ensuring the security of even the remotest end user falls under the purview of the central command. Moreover greater emphasis lies on protecting the establishment against internal threats. Later in this chapter a detailed comparison of the fundamental differences between the architectures of commercial and closed IT organizations has been provided.

2.2 Common Architectures in Closed IT Organizations

The architectures of closed IT organizations are based on the basic principle of doing it yourself. From the provision of equipment to the end user and its connectivity, to the development of applications for maintaining their services, closed organizations do everything on their own. This principle infuses some basic variations in their IT architectures as compared to commercial enterprises, as clarified by the diagram below.

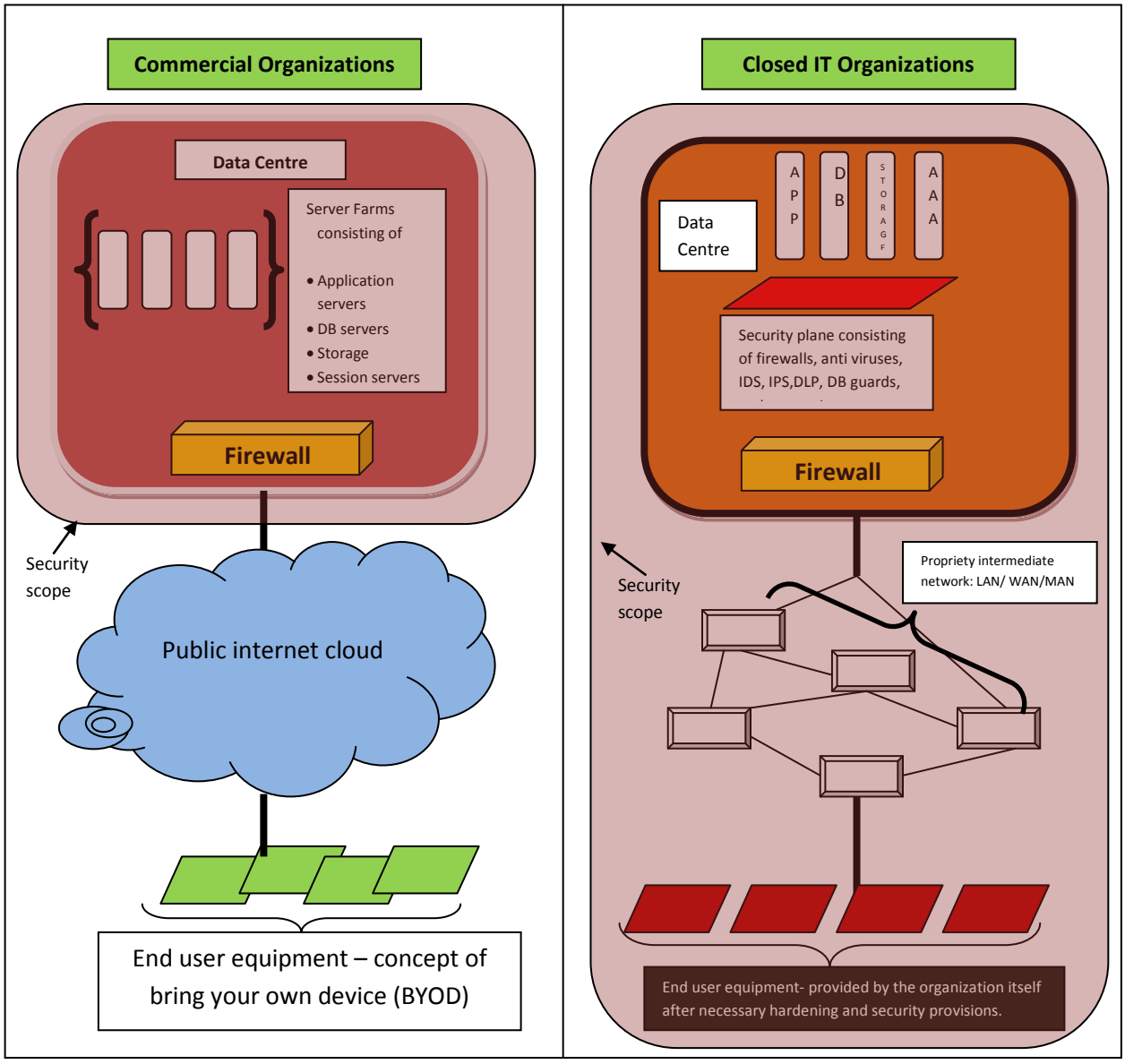

Fig.4: Generic IT Architectures of Closed IT Organziations

It can be noted in the above mentioned diagram that the scope of central command for providing security, in closed IT organizations, extends to the end user also, whereas commercial organizations are concerned with securing their Data Centre assets only. Detailed differences between the two organizations have been elaborated in the next section

2.3 Differences between Commercial and Closed IT Organizations' Architectures

Due to the fundamental difference in the security objectives of both organizations, the architectures of closed IT organizations are different in their nature as compared to their commercial counterparts. In closed organizations, more emphasis resides on the factor of confidentiality and secrecy. Internal threats are much more significant than any external danger. Resultantly closed organizations tend to develop their propriety applications to serve their needs, instead of procuring off the shelf solutions. Moreover their security paradigm extends till the last mile connectivity. Almost all services and equipment installed in closed organizations is self managed whereas in commercial enterprises several of their critical functionalities are outsourced for the obvious reasons of cost benefit. The table given below summarizes these differences:

Sno	Commercial Enterprises	Closed IT Organizations
1.	Off the shelf commercial products	Indigenously developed applications
2.	Last mile connectivity and end user eqpt is out of concern	Owners and providers of complete architecture right from server farms to last mile end user eqpt and his security
3.	More emphasis on outsider threats	Greater emphasis on insider threats
4.	Large number of services outsourced	Self managed
5.	More worried about availability	Confidentiality is the first priority
6.	Have limited resources when it comes to implementing security for the reason of cost benefit.	Earmark extensive resources for providing security.

Table.1: Differences between Commercial and Closed IT Organizations

These differences give rise to a unique threat canvas for closed organizations.

2.4 Summary

Due to different business and security objectives being followed by closed and commercial enterprises, their architectures and threat canvases are also dissimilar, which gives rise to the need of having a separate framework or methodology for implementing security solutions in both. All those instances where commercial standards and procedures have been blindly implemented in closed organizations, without any fine tuning or customization, acute deficiencies have been experienced and the security paradigm has failed to achieve its desired results.

THE CONCEPT OF SECURITY OPERATIONS CENTRE (SOC)

The phenomenon of Security Operations Centre is not relatively new, however during the last decade, exponential advancement in cyber attack techniques has brought this concept to limelight. Despite employing state of the art IT security measures, organizations in general and sensitive organizations in particular are resorting to obtain the services of SOC, io order to monitor their complete security and operational posture from one screen.

3.1 Definition

SOC is an organization consisting of people, processes and technology which is established to monitor all security related events from enterprise IT assets including both security assets as well as operational devices[1]. The assets may include everything ranging from servers and applications to firewalls, IDS, IPS and networking devices. SANS institute gives a concise diagrammatic definition of SOC as follows[6]:

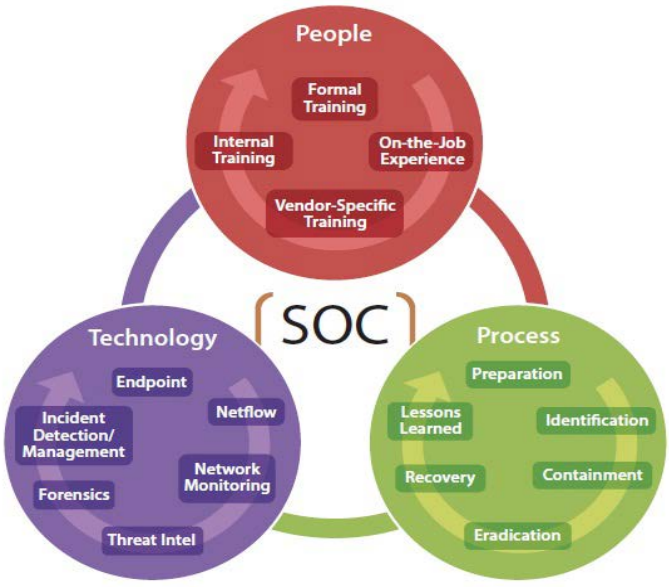

Fig.5: SANS Institute Definition of SOC [6]

3.2 The Concept (Why is SOC Required)

In order to protect themselves from possible cyber threats, data breaches and information compromises, organizations have been employing state of the art IT security mechanism, including anti-viruses, firewalls, IDS, IPS, DLP, Data guards, encryption e.t.c. These mechanisms are usually employed in security layers, spanning over the complete layers of the OSI model. However, despite such stringent security measures and their deliberate applications, the incidents of cyber attacks have experienced a monumental increase over the past five years, as signified by the statistics quoted in the introduction. The prime reason for the failure of these measures, in containing cyber threats, was the fact that although these mechanisms were employed as complete solutions within themselves, they tended to operate in isolation with each other when employed in an overall IT architecture. Each mechanism worked on its own and tried to stop the threat at its own end, thus giving rise to the phenomenon of security silos. There was no central mechanism that could gather events, intelligence and security status from all security devices and present a holistic, coherent picture of the threats being developed within the organization, to the security administrators. This gave rise to the need of SOC, a mechanism which could monitor the security devices in real time and obtain feed from them to present an intelligent view of the organization's security posture at any given moment. Initially SOC was restricted to monitoring events and incidents from security related devices only. However as the concept matured over years, it included monitoring of operational devices also. Now, an ideal deployment of SOC, keeps a vigilant watch on the complete IT architecture for security related incidents and provides its organization a with a proactive reaction capability to deal with cyber attacks.

3.3 Basic Functionalities Provided by SOC

Initially the mechanism of SOC was designed for monitoring only. However with the passage of time, the concept evolved into providing several other security functionalities which were related to each other, for providing effective protection to the overall IT infrastructure. Although these features were fully functional separate security tasks in themselves, but when employed coherently, they augmented each other's performance to provide a more effective

security solution to the organization. These additional functionalities included the feature forensics, incident response (IR), penetration testing and compliance and audit.

3.4 Basic Architecture of SOC

An ideal SOC which consists of all the above mentioned functionalities has an architecture as shown in the following figure:

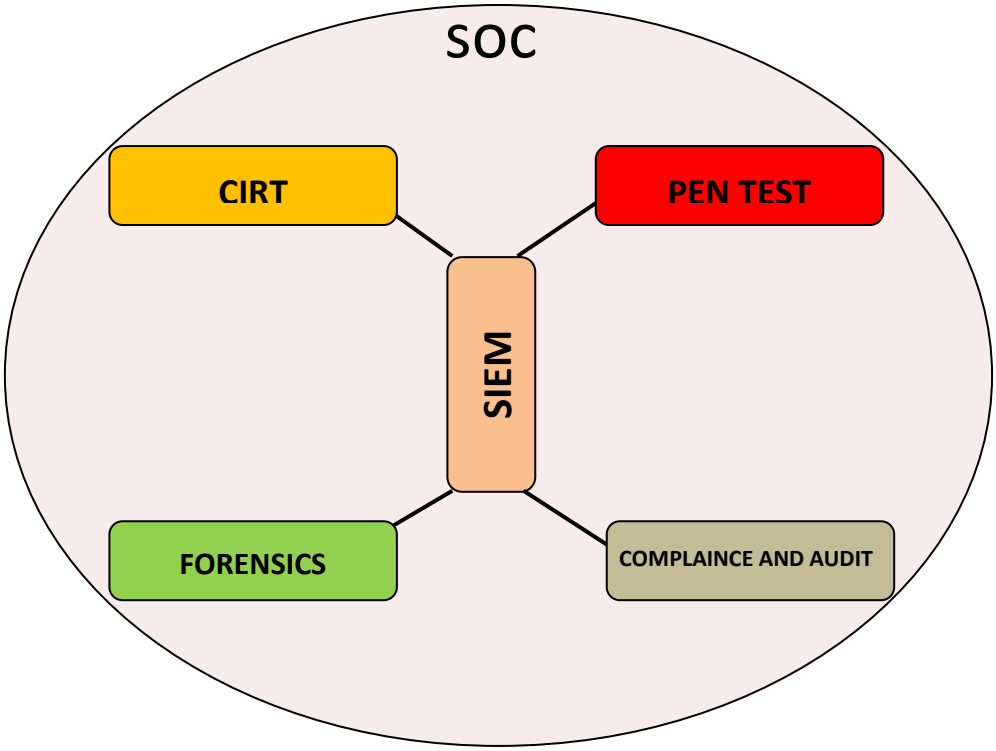

Fig.6: Basic Architecture of SOC

3.4.1 SIEM (Security Information and Event Management)

SIEM forms the backbone of any SOC. It is a software tool that is integrated, maintained and monitored round the clock by a dedicated, structured team of human resources. The main functionality of SIEM is to collect feed from all security and operational devices, within an IT architecture, in the form of event logs and flows. This feed is then parsed into a common format and compared against a set of rules, to pronounce whether a violation of IT security policy or breach of data has taken place or not. These rules are based on the overall IT security policy of

the organization and are created inside the SIEM software by the technical resources managing it. Thus SIEM is that single point which collects and converges information from all devices and coverts it into intelligence. All other components of SOC either depend on it or take help from it, thus it is termed as the backbone of SOC.

3.4.2 CIRT (Cyber Incident Response Team)

Whenever an incident or attack is highlighted by SIEM, the first group of people which reacts to mitigate the subject attack or incident is the Cyber Incident Response Team. In the event of a security offence, it is forwarded to CIRT which contacts the operational administrators of the concerned section or sub organization and guides them as to what all actions to take in order to mitigate the offence. CIRT could be termed as the quick reaction force of a SOC.

3.4.3 Forensics

A well established SOC contains a dedicated team which is skilled in performing log forensics on various incidents. All chronological data pertaining to incidents and offences, is made accessible to the forensic team, which expertly analyzes it to dig out the real reasons for the offence and to decide as to who or what is responsible for the subject violation. A skilled forensic team will also predict any attack which is in the process of developing slowly and stealthily, i.e. advanced persistent threat. The members of a forensic team in SOC should be experts of reading and interpreting human intentions from logs and packet flows, apart from having an in depth knowledge of the functioning and flow of complete IT architecture of the organization. They should preferably be experienced domain administrators who have been trained and promoted to be a part of forensic team.

3.4.4 Pen Test

Penetration testing team, in short pen testers form the most vibrant part of SOC. It is the responsibility of this team to continuously conceive, simulate and launch all possible cyber attacks that could be carried out on the organization by an attacker, and probe into any loopholes that have been left unplugged. The pen test team plays a very vital role in fine tuning the overall security mechanisms of the enterprise, as well as improving the performance of SOC. The team

members need to be expert in penetration testing skills and should have the capability to think in unconventional ways, so that they can predict the future moves of the attacker [2].

3.4.5 Compliance and Audit

The fifth functionality of SOC is provision of a dedicated compliance and audit team. The mandate of this team is to ensure that whatever IT security policies, which have been defined by the executive authorities of the organization, are being implemented in true letter and spirit. It carries out periodic audits to check and certify the organization or sub organizations for compliance. Moreover it also keeps a watch on the vulnerabilities that exist in the system or are introduced afresh due to some operational activity. In this regard the compliance and audit team conducts regular vulnerability scans of the complete architecture [2].

3.5 Summary

The concept of SOC is important when it comes to providing proactive threat intelligence and the status of IT security posture of an organization, at any instant. However establishing a successful SOC is not a one day task. It requires certain basic functionalities to be present and developed dedicatedly over time, before a SOC can be expected to efficiently achieve its objectives.

Chapter 4

LITERATURE REVIEW OF EXISTING SOC FRAMEWORKS

Substantive research on the design and modalities of Security Operations Centre has been conducted in the past decade. However most of this research has been carried out keeping in mind the commercial requirements of IT industry or it has been vendor and product specific [2]. Moreover, whatever few frameworks that have been proposed, they deal with the design aspect of SOC only and the aspect of establishment or maintenance of SOC is not addressed. This chapter provides a concise overview of what all other researchers have written or proposed in relation to SOC.

4.1 Basic Building Blocks of SOC

SANS Institute of IT Security, in its white paper [6] defines SOC as a combination of people, processes and technology.

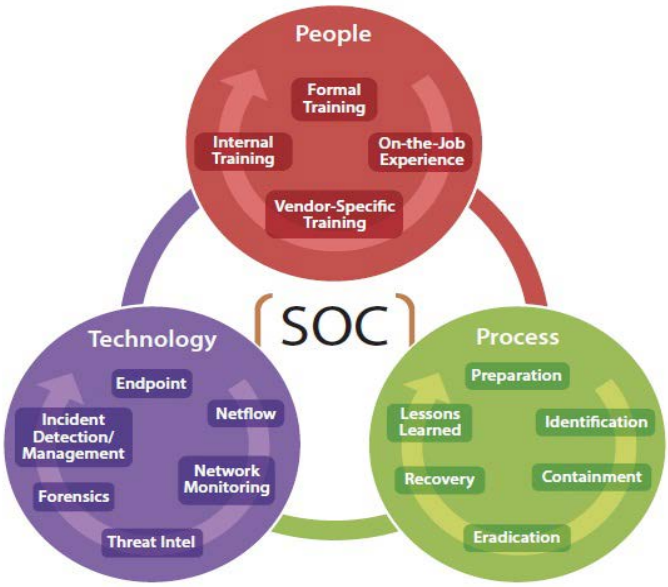

Fig.7: Basic building blocks of SOC [6]

According to the subject white paper, these three features form the building block of any SOC and to handle and manage them effectively the human resource should be divided into various tiers as shown in the following table:

Job Title	Duties	Required Training
Tier 1 Alert Analyst	Continuously monitors the alert queue; triages security alerts; monitors health of security sensors and endpoints; collects data and context necessary to initiate Tier 2 work.	Alert triage procedures; intrusion detection; network, security information and event management (SIEM) and host-based investigative training; and other tool-specific training. Certifications could include SANS SEC401: Security Essentials Bootcamp Style.
Tier 2 Incident Responder	Performs deep-dive incident analysis by correlating data from various sources; determines if a critical system or data set has been impacted; advises on remediation; provides support for new analytic methods for detecting threats.	Advanced network forensics, host-based forensics, incident response procedures, log reviews, basic malware assessment, network forensics and threat intelligence. Certifications could include SANS SEC501: Advanced Security Essentials - Enterprise Defender; SANS SEC503: Intrusion Detection In-Depth; SANS SEC504: Hacker Tools, Techniques, Exploits and Incident Handling.
Tier 3 Subject Matter Expert/ Hunter	Possesses in-depth knowledge on network, endpoint, threat intelligence, forensics and malware reverse engineering, as well as the functioning of specific applications or underlying IT infrastructure; acts as an incident "hunter," not waiting for escalated incidents; closely involved in developing, tuning and implementing threat detection analytics.	Advanced training on anomaly-detection; tool-specific training for data aggregation and analysis and threat intelligence. Certifications could include SANS SEC503: Intrusion Detection In-Depth; SANS SEC504: Hacker Tools, Techniques, Exploits and Incident Handling; SANS SEC561: Intense Hands-on Pen Testing Skill Development; SANS FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques.
SOC Manager	Manages resources to include personnel, budget, shift scheduling and technology strategy to meet SLAs; communicates with management; serves as organizational point person for business-critical incidents; provides overall direction for the SOC and input to the overall security strategy.	Project management, incident response management training, general people management skills. Certifications include CISSP, CISA, CISM or CGEIT.

Table 2. Human Resource Tiers for Operating SOC [6]

However SANS institute considers that only a SIEM solution and its associated manpower make up a SOC, and do not talk about the other four functionalities mentioned in chapter 3 of this thesis.

Steif Schinagl, Keith Schoon and Dr. Ronald Pans in their paper [2] describe SOC as a combination of five basic functions along with several sub functions that are extended to support the operations of SOC, as described in the following figure:

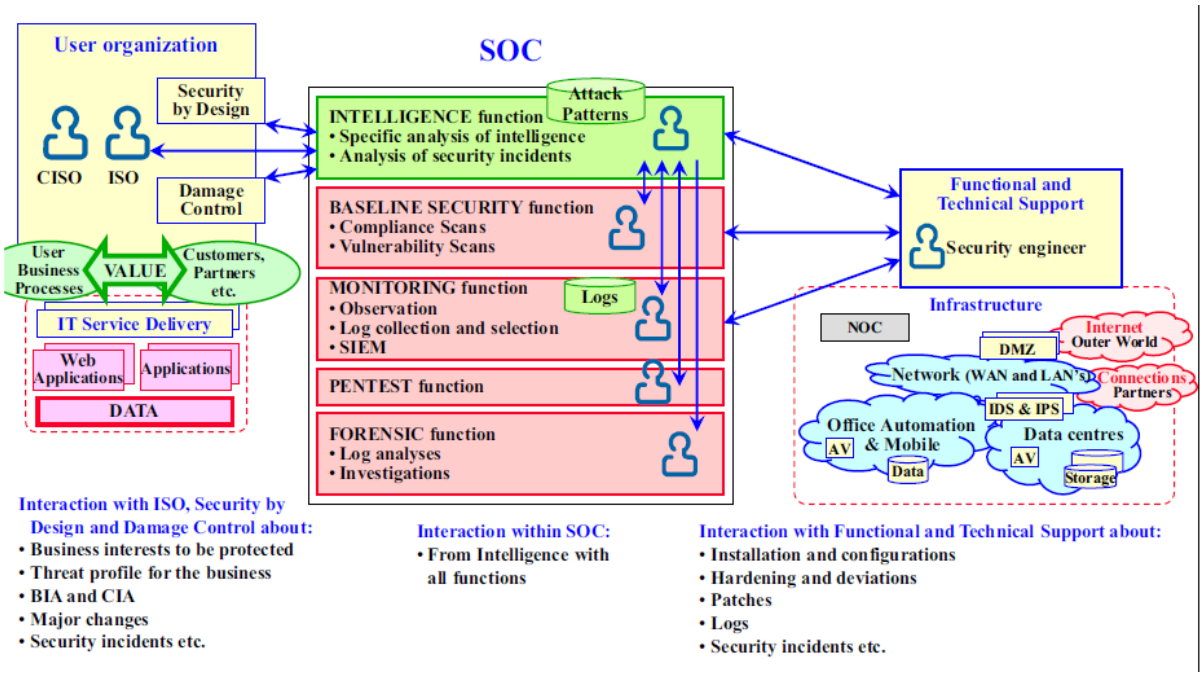

Fig 8. Design of SOC [2]

The subject paper describes how SOC is designed and what all functions it can perform. But it does not touch upon what process to follow in order to successfully establish this architecture of SOC. Moreover it describes the functions of SOC, keeping its pure commercial usage in mind, whereas SOC is equally employed in private sensitive organizations which have a different set of requirements when it comes to implementing Security operations Centre.

4.2 Establishment Processes of SOC

A white paper published by McAfee [5], describes the process of establishing SOC as a combination of seven steps as follows:

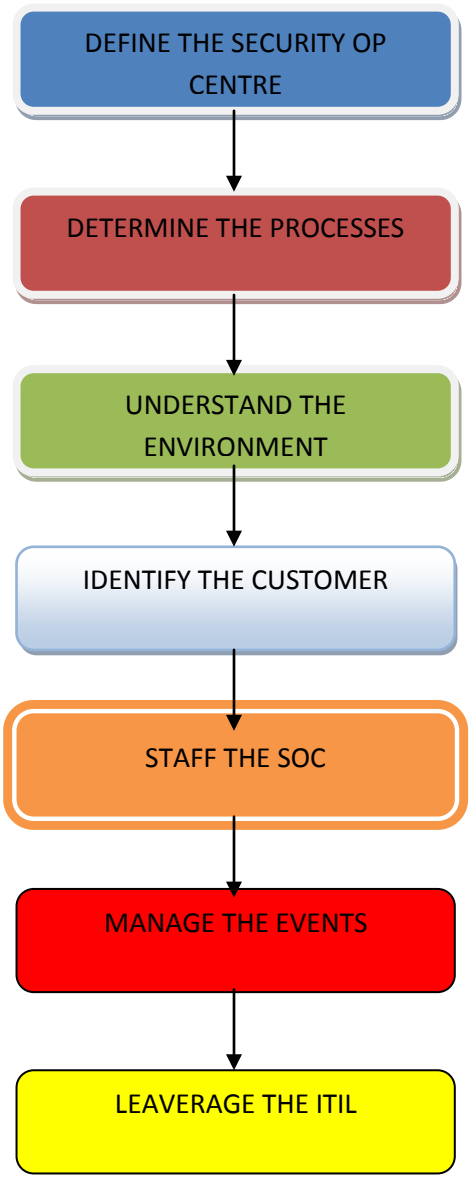

Fig 9. MACAfee's White Paper on Establishing SOC

The process of establishing SOC, defined in MACAfee's white paper, does not take into consideration the organizational security goals and policies. Moreover it has more emphasis on how to manage the staff which is running SOC rather than how to ensure efficient deployment of SOC so that coherence between people, processes and technology could be obtained. Even further, this framework is again developed for a commercial SOC which is established to provide

outsourced SOC services to its clients on payment. It is inappropriate to apply this framework on private sensitive organizations which have a different objective for SOC.

4.3 Challenges Faced by SOC

Loi zomlot and Sandeep Bhatt of HP laboratories beautifully explain the concept of SOC in their paper [1] and the challenges faced by this organization. They take SOC as a log collecting mechanism with just two functions, monitoring and forensics as depicted in the following figure

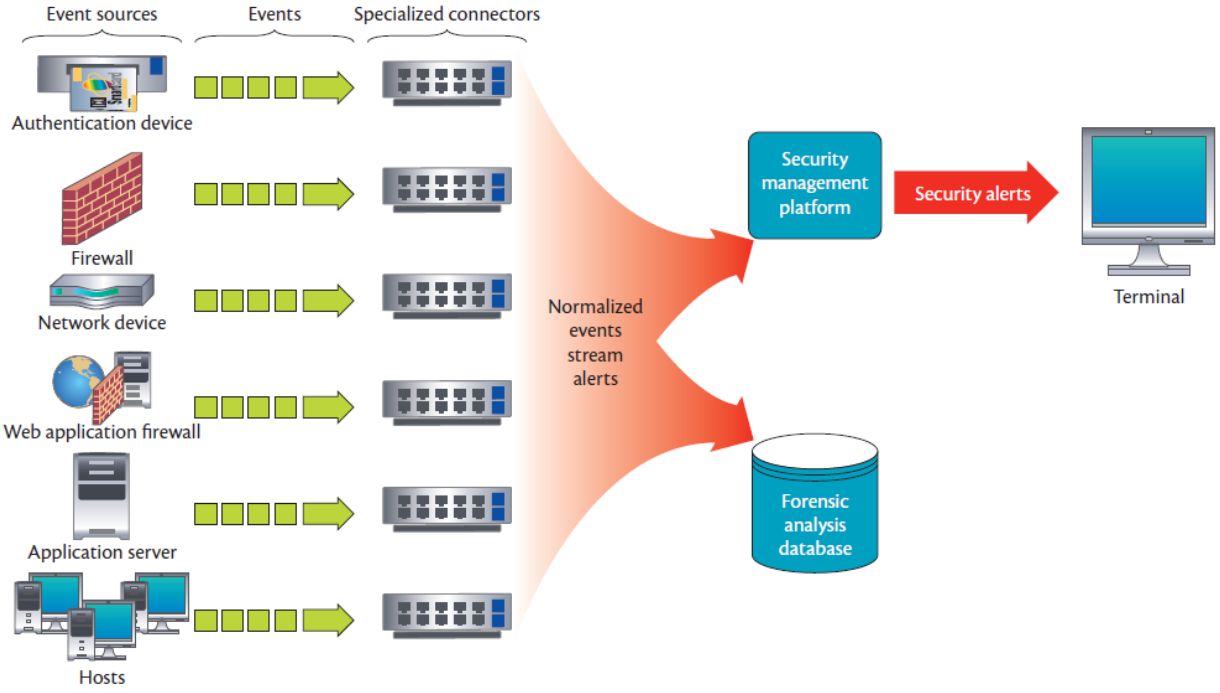

Fig 10. Functionality of SOC [hp]

They explain that SOC is an organization which has its resources divided into three levels of expertise as follows

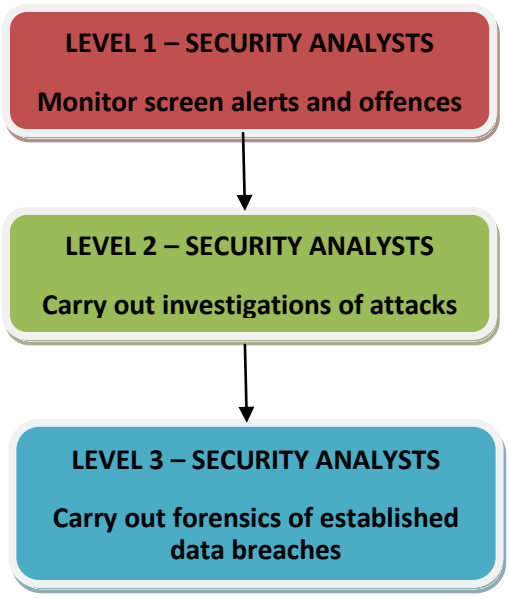

Fig 11. Levels of SOC s Technical Resources

Moreover, they explain the challenges faced by any SOC organization which include:

- The Technical challenge of efficient rule creation and management.
- Handling of large number of false positives and false negatives.
- Lack of contextual intelligence or information sharing between various sections of SOC itself and between SOC and Operations team.
- Problems with event collection, co-relation and analysis.
- Challenges of efficiently interpreting human intention from log data analysis.
- Dearth of trained manpower.

4.4 Summary

A literature review, of the efforts of previous researchers on defining the process and design of SOC, reveals that whatever little frameworks have been suggested till date are mostly formulated keeping commercial objectives in mind. Moreover nearly all of them deal with the design architecture of SOC or management of its HR. Still a lot more work needs to be carried out on how to efficiently establish a SOC and what all best practices to follow so that SOC can fulfill its desired objectives successfully.

Chapter 5

THE PROBLEM STATEMENT

Since the security objectives being followed by private sensitive organizations are very different in their nature as compared to their commercial counterparts, as already highlighted in Chapter 3, the IT architectures developed for such closed Organizations are also different in their goals and functionality. This diversity, in the nature of architectures and aims trickles down to the establishment and running of SOC also.

5.1 Problem with Existing Frameworks of SOC

As discussed in previous chapters, whatever little frameworks that have been developed for SOC, are based on satisfying commercial requirements of the industry [2]. They have a greater focus on the design of SOC or its management. These commercial frameworks, when implemented in closed IT Organizations are found to be out of line, inadequate and lacking in fulfilling their desired objectives or goals, for the prime reason that they do not take into account the differences of both organizations. Moreover it is very seldom that we find a comprehensive guideline on what all sequential steps to follow in order to establish a successful, customized SOC.

5.1.1 Why Existing Frameworks of SOC are Inadequate for Closed IT Organizations

There are several glaring reasons, why we cannot achieve our desired results from SOC, when we use commercial frameworks to establish and run this mechanism in closed IT enterprises:

- Due to difference in IT architecture, its nature and security objectives, closed IT organizations have a different threat canvas in comparison to commercial concerns. In closed organizations more emphasis lies on mitigating internal dangers than external threats. Secrecy of information assumes prime importance. The available SOC frameworks in the market do not take into account their peculiar threat canvas and are based on generalized industry specific threat intelligence [2].
- The existing SOC frameworks are so designed that they have more emphasis on providing outsourced security services to their client organizations whereas in sensitive

organizations there is no concept of outsourcing. Even the last mile connectivity and end user equipment is provided by the central authorities.

- The security paradigm of closed IT organizations extends up to the end user and it is the responsibility of the centre to ensure the secrecy of every user also, which forms an internal part of the organization, as described in chapter 3. Existing SOC frameworks do into take this into account.
- SOC literature available in the market is mostly vendor specific and aims to satisfy common industry standards such as PCI-DSS, HIPPA, COBIT, ISO standards e.t.c. These industry standards are mostly not completely applicable in the environment of closed IT enterprises.
- Guiding frameworks of SOC, available in the market are somewhat generalized in nature [2] and do not streamline the finer implementation concerns and points, which should be followed to establish an effective SOC mechanism. These frameworks leave the implementation steps to the imagination of human managers who can have very diversified assimilation about any single goal.
- Given the criticality of data security in closed IT Organizations, the luxury of leaving the establishment procedure to the understanding and imagination of human managers cannot be afforded. No streamlined custom made procedure exists in the market which deals with the requirements of sensitive private organizations in specific.

The above mentioned factors give rise to the requirement of our thesis which is stated in the succeeding paragraph

5.2 The Problem Statement

To formulate a standard framework for establishing and maintaining SOC, which should be crafted to the specific security needs and threat canvas of closed IT Organizations.

5.3 Summary

This chapter summarizes the problems being experienced with existing SOC frameworks when implemented in private sensitive organizations and describes the problem statement of this thesis in a single sentence.

Chapter 6

RESEARCH AND EVALUATION METHODOLOGY

The research and evaluation, conducted in pursuance of the subject thesis was divided into six steps, shown as follows

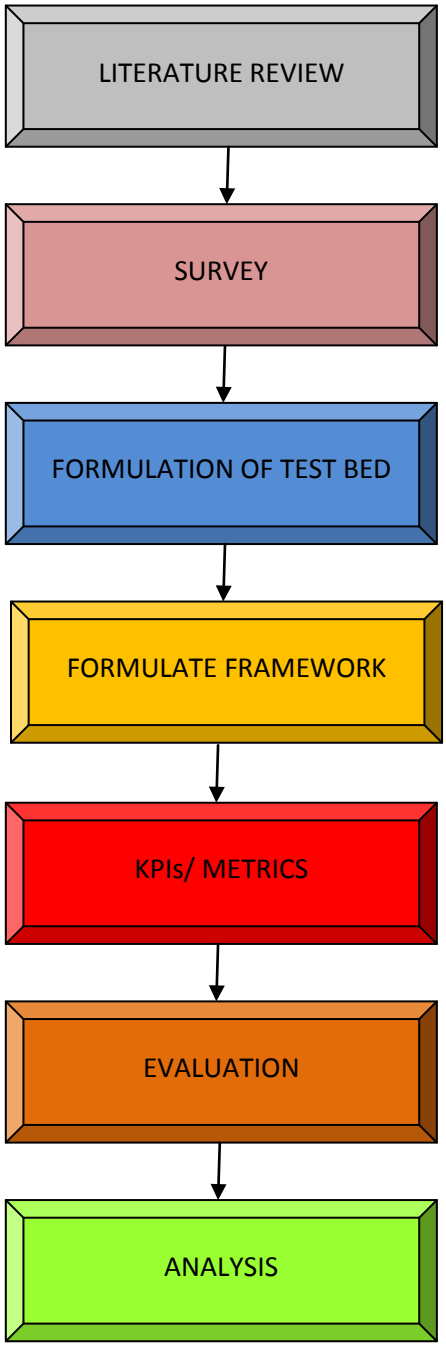

Fig .12 Stages of Research

6.1 Literature Review

In order to find the existing frameworks of SOC, that are in vogue in the market and to discover what work has already been contributed by other researchers, an extensive literature review was conducted consisting of several publications both IEEE as well as vendor specific. Moreover, a thorough study of industry based research on SOC was carried out to get a firsthand knowledge of what all standards of SOC are being followed in the market and whether any of those standards already fulfill the requirements of private sensitive organizations, termed as closed IT organizations in this thesis. A detailed list of the literature, reviewed during the course of our research has been shared in the bibliography.

6.2 Survey

In order to confirm the initial understanding of the subject problem, which was formulated as a result of the literature review conducted, a detailed survey of five large private organizations was carried out. Each of these enterprises satisfied the definition of closed IT organization and was in possession of a sizeable Security Operations Centre. The survey consisted of a questionnaire which was presented to the IT authorities of each organization and their replies were noted down in order discover how they implemented their SOCs what all flaws and problems they faced while achieving their desired objectives from the said mechanism. The questionnaire consisted of following questions:

- **Question 1**. While establishing SOC did you follow any framework or deployment method? If yes which one?
- **Question 2**. Does your organization have an overall IT security policy?
- **Question 3**. Does your organization have a SOC operational policy?
- **Question 4**. Before employing SOC was any risk analysis of assets and their categorization according to importance was carried out?
- **Question 5**. During the deployment of SOC what problems did you face ?
- **Question 6**. After the SOC was deployed and functional what problems are you facing now?
- **Question 7**. Are all devices being monitored or some have been left out ?
- **Question 8**.While selecting your SIEM tool, on what criteria did you evaluate your tool ?
- **Question 9**. What number of manpower did you employ in SOC? How did you decide on this number? Do you follow any structure in SOC manpower such as operators and analysts?

- **Question 10**. Did you face any resistance from the administrators and operations people while deploying SOC?
- **Question 11**. Do you have any devised reporting and response mechanism ? When an incident takes place how do you inform it to the concerned authorities ?
- **Question 12**. Do you have any feedback mechanism from the users side?
- **Question 13**. Do you have defined authorities as to who can order what ?
- **Question 14**. Do you have any training plans or knowledge criteria for the human resource. If yes what all factors does it cover ?

6.3 Formulation of Test Bed

As a result of the above mentioned steps, the actual nature of problems, in implementing SOC in closed IT Organizations, was understood and an outline framework was developed which could form the basis of resolving them. However this framework needed to be confirmed in actual functional IT environment for evaluating its effectiveness and workability. This led to the formulation of a test bed, consisting of all basic devices that are utilized in creating an IT environment of a closed IT organization. The test bed was created on a hybrid of virtual and physical platform and was a small scale replication of the actual environment, however all endeavors were made to make it as near to reality as possible (Figure 12).

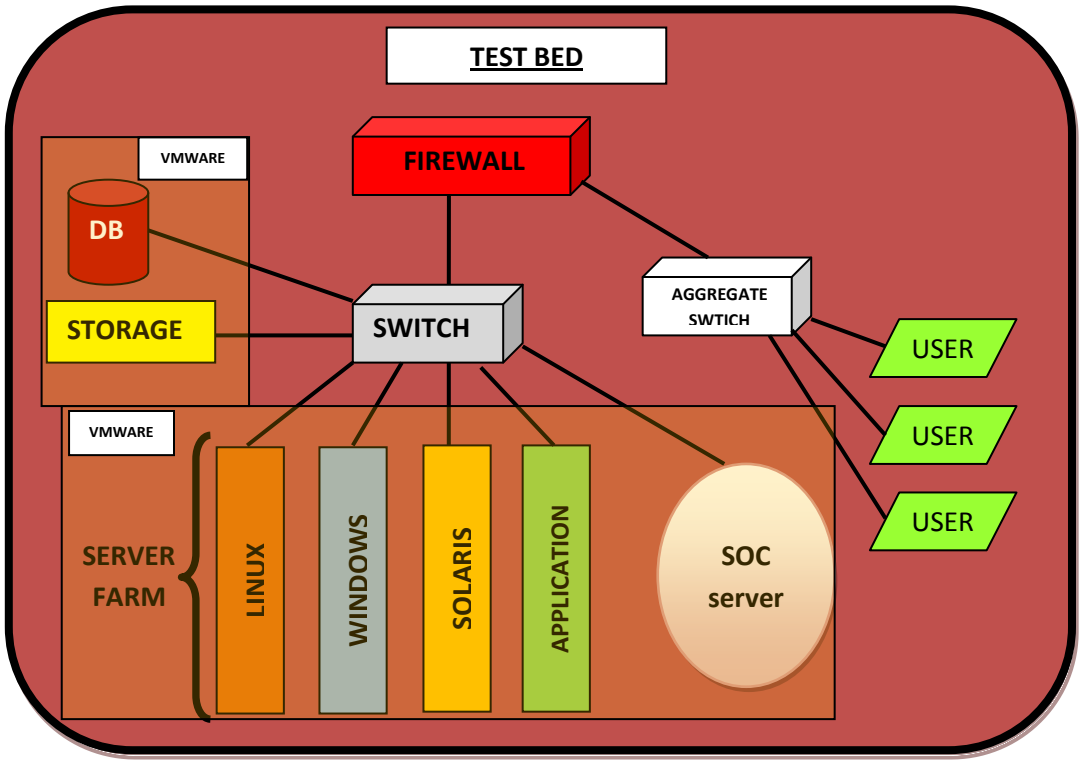

Fig.13 Test Bed Architecture

6.4 Key Performance Indicators (KPIs) / Metrics

In order to obtain substantial evidence about the effectiveness and workability of the proposed SOC framework, an extensive research was conducted on the key performance indictors or metrics that are currently being used in the market to evaluate SOC. Out of numerous KPIs only the relevant and concerned were shortlisted and noted for further utilization. These KPIs were divided into two categories i.e. qualitative and quantitative as shown in the following tables.

Qualitative KPIs

Ser	KPI (Metric)
1.	Provision of feedback within the framework
2.	Repeatable processes
3.	Provide complete linkage to the source of offence: Granularity of detection
4.	Successful creation of reporting chain
5.	Scalablility
6.	Competency development roadmap and training of human resource
7.	Periodic assessment of HR
8.	Documentation of SOC procedures and info flow
9.	Situational risk awareness
10.	Provision of intelligence peculiar to own architecture
11.	Prioritization of Targets
12.	Maintain a baseline configuration specimen
13.	Identification and auth of user activities
14.	Escalation of risk related data, reporting and anomalies
15.	Provide periodic and timely maintenance
16.	Carry out periodic risk assessment
17.	Integration between people, processes and Technology- overall security objective
18.	Provision of minimum use cases
19.	Ensure info sharing b/w Soc and Ops

Table.3: Qualitative KPIs/ Metrics[1,12,13]

Quantitative KPIs

Ser	KPI/ Metric	Formula	Maximum Good Performance Value	Maximum Bad Performance Value
1.	Attack detection accuracy	(true positives + true negatives)/ total packets	1	0
2.	False positive rate	False positives/ total packets	0	1
3.	False negative rate	False Negatives (attacks missed)/ total packets	0	1
4.	Computational Cost	Cost=(1-attack detect accuracy) +K(False positive rate) : where K=FP-FN	<1	>1
5.	Sensitivity	True positive/(true positive + false negative)	1	0
6.	Specificity	Specificity= true negative/(true negative + false positive)	1	0

Table.4: Quantitative KPIs/ Metrics

6.5 Evaluation

Once the details of the proposed framework, for the establishment and maintenance of SOC were streamlined and test bed was successfully created, an extensive evaluation was carried out of the subject framework against the KPIs mentioned in the previous section. The evaluation mechanism was different for quantitative KPIs as compared to qualitative ones.

6.5.1 Evaluation for Quantitative KPIs

For quantitative KPIs the before and after evaluation methodology was adopted. It comprised of collecting data values from the test bed, before the implementation of framework features. Once this data set was complete, the framework was implemented in true letter and spirit, as close to reality as possible, after which another set of data values was collected. Both these sets were compared to each other and their improvements if any were graphically depicted. The details of these results are provided in chapter 8.

6.5.2 Evaluation of Qualitative KPIs

For qualitative KPIs argumentative evaluation was used. The proposed framework was scrutinized for the presence or absence of the various features mentioned in the KPIs and corresponding arguments were presented with references to specific sections of the framework that satisfied those metrics. Results are shared in chapter 8.

6.6 Analysis

An analysis was carried out, basing on the results of the above mentioned evaluation and the framework was graded accordingly. For the purpose of grading the proposed framework, the standards and levels suggested by Hewlett Packard in their publication [11] were used. Results are shared in chapter 8

6.7 Summary

Extensive research and evaluation was conducted to confirm whether the proposed framework was effective enough to mitigate the stated problems concerning the establishment and maintenance of SOC in closed IT Organizations. Basing on this evaluation, the subject framework was graded according to the accepted industry standards.

Chapter 7

PROPOSED FRAMEWORK FOR SOC

The extensive research, survey and evaluation carried out in connection to this thesis resulted in the formulation of a detailed and granular framework, for the establishment and maintenance of SOC in Closed IT Organizations. The framework was developed with the sole aim of addressing the problems and peculiar threat canvas of closed organizations, when it came to establishing and running their security operations centre. During the process of analyzing and solving the stated problem, certain primly important features were identified which should have formed a necessary part of the proposed solution. These features translated into goals of the subject framework described as follows.

7.1 Goals of the Proposed Framework

The framework was designed, for closed IT organizations, with following goals in mind

- Propose an organizational structure/ design of SOC.
- Propose a comprehensive and granular establishment framework.
- Formulate criteria for selection of SOC tools.
- Devise a basic set of minimum required intelligence to be obtained from SOC.
- Propose a human resource infrastructure to run and maintain SOC.

7.2 The Proposed Framework

The salients and details of the proposed framework are discussed as under

7.2.1 Proposed Organizational Structure of SOC

The basic design or structure of SOC, to be utilized in closed IT Organizations is to consist of the same functionalities as being used in standard market practice and already defined in chapter 3. However these functionalities need to be established and implemented in a method which specifically addresses the problems of closed organizations. The organization of SOC should consist of five basic functionalities, namely SIEM, Forensics, CIRT, Pentest and Compliance and Audit (figure 13)

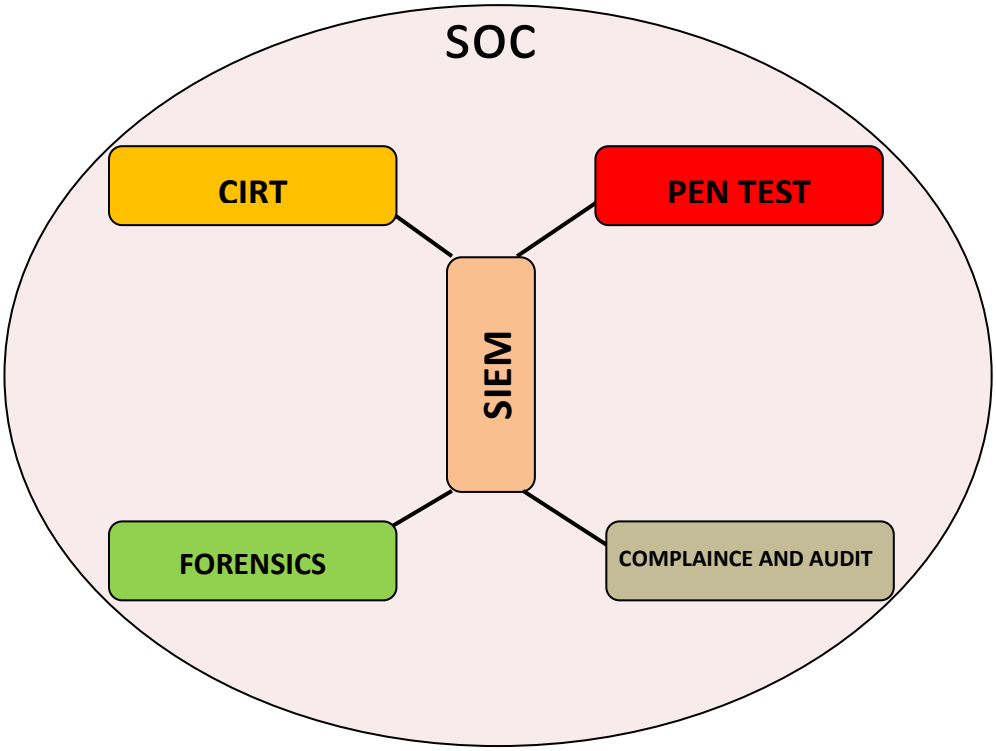

Fig 14. Basic Design of SOC

7.2.2 The Establishment Framework

The process of establishing and maintaining a SOC has been divided into four recurring phases as shown in figure 14.

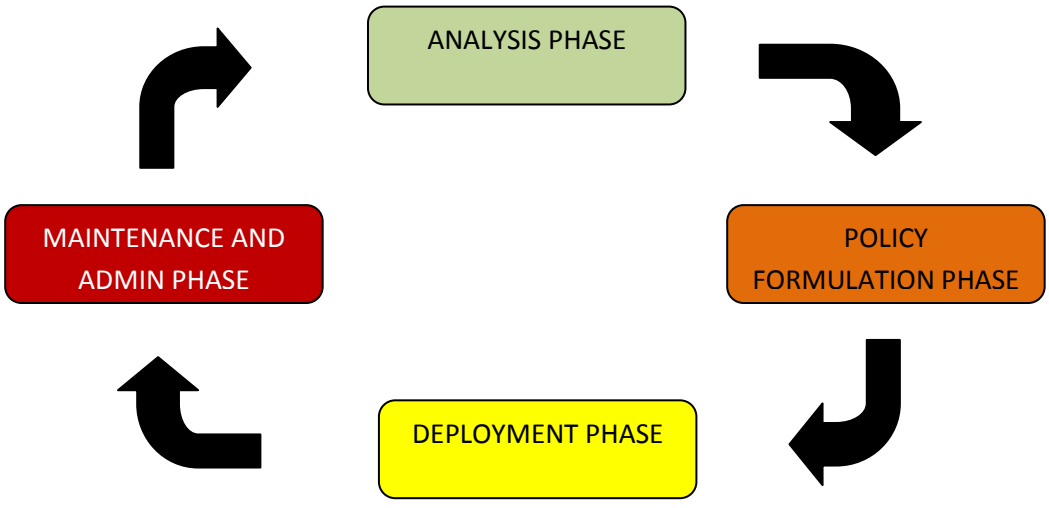

Fig 15. Phases of SOC Framework

7.2.3. The Analysis Phase

The analysis phase consists of all the steps which will provide a sound base or homework for establishing and running an efficient Security Operations Center (SOC), within the organization. These steps may appear trivial at the start but each one of them is indispensible in itself, since all the further deployment and decision making is based on them. An overview of the steps involved in the analysis phase is shown as follows:

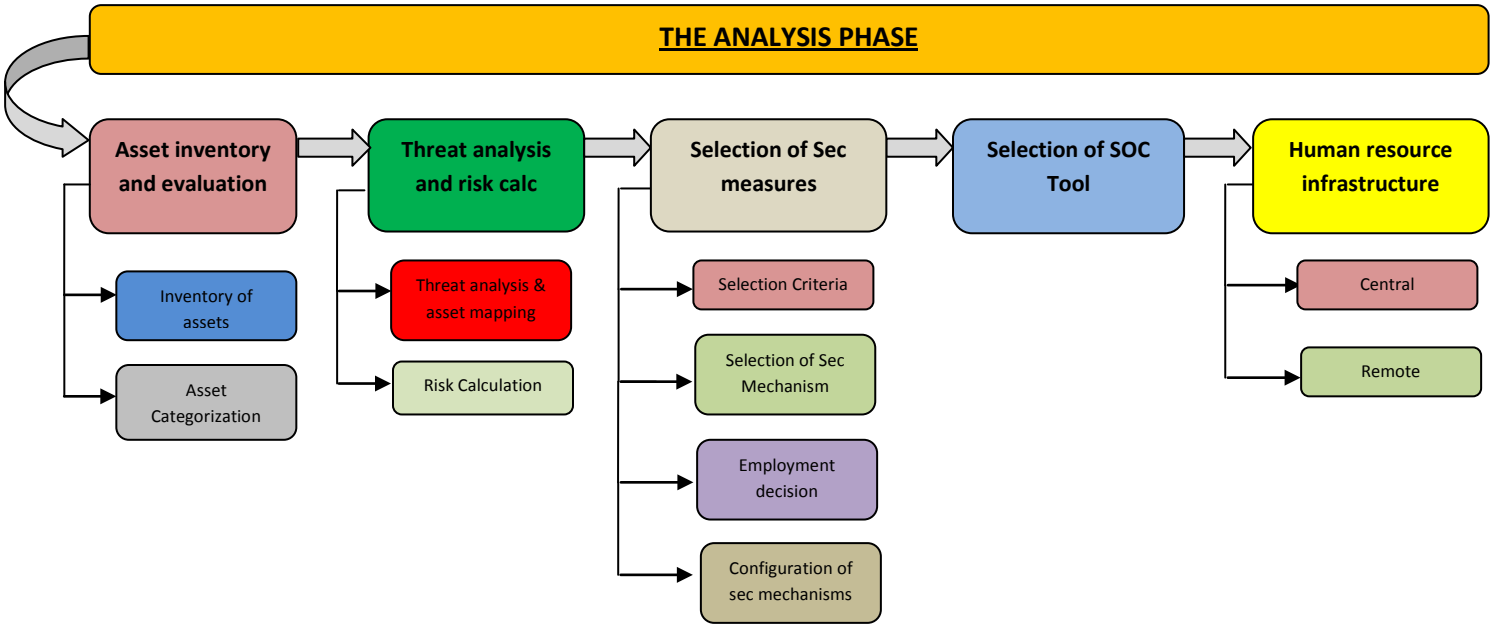

Fig 16. The Analysis Phase

7.2.3.1 Asset Inventory and Evaluation.

Any organization cannot achieve the desired objectives from its SOC/ SIEM till the time it exactly does not know what all it has to monitor and against which all threats. Keeping this in mind the logical steps that are required to be carried out in asset inventory and evaluation are as follows

1) Inventory of Assets. List down and account for each and every asset that is installed in Data Centers, or the regional offices/ sub offices.

The assets are not limited to but include all of the following

- All network devices
- All hardware servers
- All operating systems
- All applications (custom made/ commercial off the shelf)
- All database instances
- All storage devices

2) **Specimen table**. A specimen table for listing of assets is given at table 1, as a guideline for the resources carrying out the task.

Domain			(Networks, windows, solaris, e.t.c)	
Ser	**Device**	**Unit/ loc in DC**	**IP**	**OS**

Table 5: Asset Inventory Table

3) **Asset Categorization**. This step involves determining the relative importance of every asset compared to each other and to the overall architecture in totality. This importance is determined by evaluating each asset against the criteria of confidentiality, integrity and availability. The evaluation is carried out by brainstorming what adverse effect will take place in the IT operational environment if the confidentiality, integrity and availability of a particular asset is compromised. A particular number on a scale of 1 to 10 (1 being the lowest and 10 being the highest) is assigned to each asset in the list against compromise of confidentiality, integrity and availability column. After the completion of this numbering for one asset the average of three numbers is calculated and noted down in the table. This number gives the overall importance of the asset to the architecture. The higher the number against an asset, the more critical it is to the architecture and the more adverse affects its compromise will have on the IT operations. The exact procedure can be carried out as follows:

- Evaluate each asset against three factors that determines how important an asset is – if an element is compromised for confidentiality, integrity and availability how badly will it bog down the system – the CIA triad.

- List the assets in the descending order of importance after determining the overall impact factors for each asset.

- Specimen table. A specimen table for the subject activity is provided in table 2 as a guideline.

Ser	**Asset**	**Impact Factor (if compromised) Scale: 1-10**			**Final Impact factor**
		Confd	Integ	Aval	

Table 6. Asset Categorization Table

7.2.3.2 <u>Threat Analysis and Risk Calculation</u>.

In order to know what to monitor you ought to know which all possible ways a penetrator can attack you. Then basing on your existing architecture and security measures in place you decide which asset is likely to be effected and how badly. Following sequential procedure helps this evaluation.

1) <u>Threat Analysis and Asset Mapping</u>. This step involves brainstorming all the possible threats that can endanger the assets in particular and the overall system, and then stating as to which all assets those threats are applicable to, keeping in mind the overall architecture of the organization. It is carried out in the following sequence:

- Brainstorm all possible threat and attack vectors. Shortlist those scenarios which could endanger the system.

- The scenarios may be divided into

(a) Internal threats

(b) External threats

- Mapping of threats to assets.

(a) Decide which threats could endanger which assets.

(b) May be divided into two categories

i. Direct

ii. Indirect

- The overall architecture will dictate the final verdict as to which threat or attack is applicable to which asset.
- This mapping should be carried out in the order of importance of assets, decided in the previous step.

- **Specimen table**. For the guidance of the readers a specimen table is appended as table 7

Ser	**Assets (In the order of importance obtained from the previous step)**	**Applicable threats**	
		Direct	**Indirect**
1.			

Table 7: Threat Asset Mapping

2) **<u>Risk Calculation</u>.** In this step the probability of each threat being materialized is ascertained and then the risk faced by the corresponding assets is calculated. The procedure is as follows

- Basing on the current architecture and sec mechanisms in place, ascertain what the likelihood of each threat being materialized is.

- This likelihood is graded on a probability scale of 0 to 1and each threat is assigned its corresponding probability of materializing. To explain the process further, suppose there is a threat that someone may wire tap the media in between an edge location and a Data Center to sniff the traffic. But certain security measures such as dedicated optical fibre between the locations and properly locked and manned ME rooms and cabinet locations can reduce the probability of this threat materializing, many fold. On probability chart it may be given a value of 0.2. On the contrary a threat against which there is no security mechanism already in place has a probability of 1.

- Calculate risk for each asset according to the following formula:

Asset Risk = Asset importance (asset impact factor: step 3) x Probability of threat (7.1)

- Specimen Tables. Specimen table for the subject activity are given as follows, as a guideline:

Ser	Threat	Mechanisms in place (if any)	Probability of materializing

Table 8: Threat Probability

Ser	Assets (in descending order)		Threats		Risk (impact factor x probability)
	Assets	Asset Impact factors	Threats	Probability	

Table 9: Asset Risk Chart

7.2.3.3 Selection of Security Measures.

Now that the organization's assets have been accounted for, evaluated for importance, analyzed for probable threats and corresponding risks calculated the next logical step is to determine what all security measures are required. This step involves not only determining the need for new security measures but also re-evaluating the existing ones for their viability according to the risk scenario ascertained in the previous step.

1) Selection Criteria. The selection of security measures required/ re-evaluated should be based upon

- What all assets are employed in the architecture?
- The existent threat vectors.
- The risks calculated.

For e.g. suppose the architecture does not employ a web based application structure. And the overall network deployment consists of dedicated optical fiber connections. Yet employing a web based Data Leakage Prevention (DLP) solution and a network DLP placed at WAN is superfluous and unwise. Security solutions are to be selected exactly according to the threats faced, the risk encountered and the assets which are facing them.

2) Selection of Security Mechanism. Select security mechanisms based on the above mentioned criteria and re-evaluate the need for existing security mechanisms. The thumb rule is "**what all needs to be stopped, what all needs to be protected**". When deciding what all security measures are required you should decide the category of solution and not the vendor. Sometimes even the most anonymous vendors can provide a product which satisfies your requirements. The catch is to satisfy your requirement and not go after brand names.

3) Employment Decision. Once the measures have been selected, the next prime decision is the place where you should employ them. A good security mechanism, which is employed at a wrong location, is as bad as not being employed at all. The location or point of their application is dictated by the overall IT architecture of the organization.

4) Configuration of Security Mechanisms. Short listing and installing a security mechanism is not the end of the game. The mechanisms have to be configured correctly. How to decide what to configure. The guidelines are as follows:

- Base/ standard configuration is dictated by the overall security and operational mechanisms' configuration policy, mentioned in later sections of this thesis, and required to be developed by the organization in the policy formulation phase.

7.2.3.4 Selection of SIEM Solution. Selection and implementation of security measures leads us to the logical stage of selecting the monitoring mechanism i.e SIEM, which forms the backbone of any SOC organization. SIEM solution should be selected basing on the following questions

- Does it support the complete infrastructure? Is it capable of reporting information from all types of assets and security measures employed in an organization?

- Does it have the capability/ flexibility of being customized according to organization's security requirements (spelled out in the organization's security policy) i.e. does it have the capacity to make rules to cater for organizations security scenario.

- Basing on our research and past on job experience, an extensive 34 points based criteria for SIEM tool selection has been devised and presented in table 10 as follows for the guidance of the user.

Ser No	Parameter	Excellent	V Good	Good	Satisfactory	Poor
		(5)	(4)	(3)	(2)	(0)
1)	**Installation**					
	a) Ease of installation					
	b) Requirements of equipment					
2)	**Integration**					
	a) Ease of integration					
	b) Completeness of Devices' support					
	c) Support for various Operating systems					
	d) Aval of Agents for Various Devices/ OS					
3)	**Performance**					
	a) Real time response/ co relation					
	b) Offense indication and management					
	c) Event Correlation					
	d) Flexibility in creating and implementing rules					
	e) Quantity of aval rules					
	f) Rules Effectiveness					
	g) Support for required Use Cases					
	h) Support for required Threat Scenarios					
	i) Handling False positives					
	j) Visibility of layer 4 flows between devices					
	k) Visibility of layer 7 flows between devices					
	l) Reports and assessments					
	m) Vulnerability assessments					
	n) Capability to support large Data					
	o) Ease/ flexibility of searching desired events					
	p) User friendly dashboards					
	q) User friendly display					
	r) Reliability					
4)	**Extra Features**					
	a) Application Monitoring					

	b) Built in response to events					
	c) Vulnerability Management					
5)	Deployment in other org					
6)	**After Sales Support**					
	a) Availability of Literature					
	b) Discussion Forums on Internet					
	c) Vendor support					
	d) Training support from the vendor					
7)	Price and Scalability					
	a) Price (compared to other SIEM solutions available)					
	b) Scalability					

Table 10. SIEM selection Criteria

7.2.3.5 <u>Human Resource Infrastructure</u>.

SOC, like all other automated IT mechanisms require human workforce, for deployment and maintenance. Therefore before going into the implementation phase of SIEM it is vitally important to decide the human resource infrastructure that would be employed for this purpose. In this step you have to decide every minute detail of the following factors:

- Who would they be,
- What would be their qualifications and credentials
- What duties they would be expected to perform.

It is desirable that to streamline this important aspect of SOC/ SIEM maintenance, a separate SOP/Policy should be drafted which should govern induction, training and duty procedures of this human resource structure. As a general guideline, the human resource structure should be organized according to the following hierarchy and the policy governing them should address the under mentioned information.

1) **Central Level**

   a) **SOC Manager**

      i. Mandate.

      ii. Skills and experience required.

      iii. Duties.

   b) **Tier 1 : Analysts**

      i. Mandate.

      ii. Duties.

      iii. Skill level required/ qualifications.

      iv. Strength required.

   c) **Tier 2: Admins**

      i. Mandate.

      ii. Duties.

      iii. Skill level required/ qualifications.

      iv. Strength required.

   d) **Tier 3: Operations Experts**

      i. Mandate.

      ii. Duties.

      iii. Skill level required/ qualifications.

      iv. Strength required.

2) **Data Centers/ Remote Locations**

a) **Operations team**

i. Mandate.

ii. Duties.

iii. Skill level required.

iv. Strength required.

b) **Response team**

i. Mandate.

ii. Duties.

iii. Skill level required.

iv. Strength required.

7.2.4 **Policy Formulation Phase**

Policies are as important to the establishment of the organization of SOC as is a constitution to the establishment of a country. It is these policies which dictate every aspect of SOC, right from the selection of security equipment to the used cases or intelligence being extracted out of SOC tools. Our survey of several large enterprises, conducted during the course of this thesis, revealed that the aspect of policy formulation is the most neglected amongst organizations. An overview of the proposed policy formulation process is shown as follows

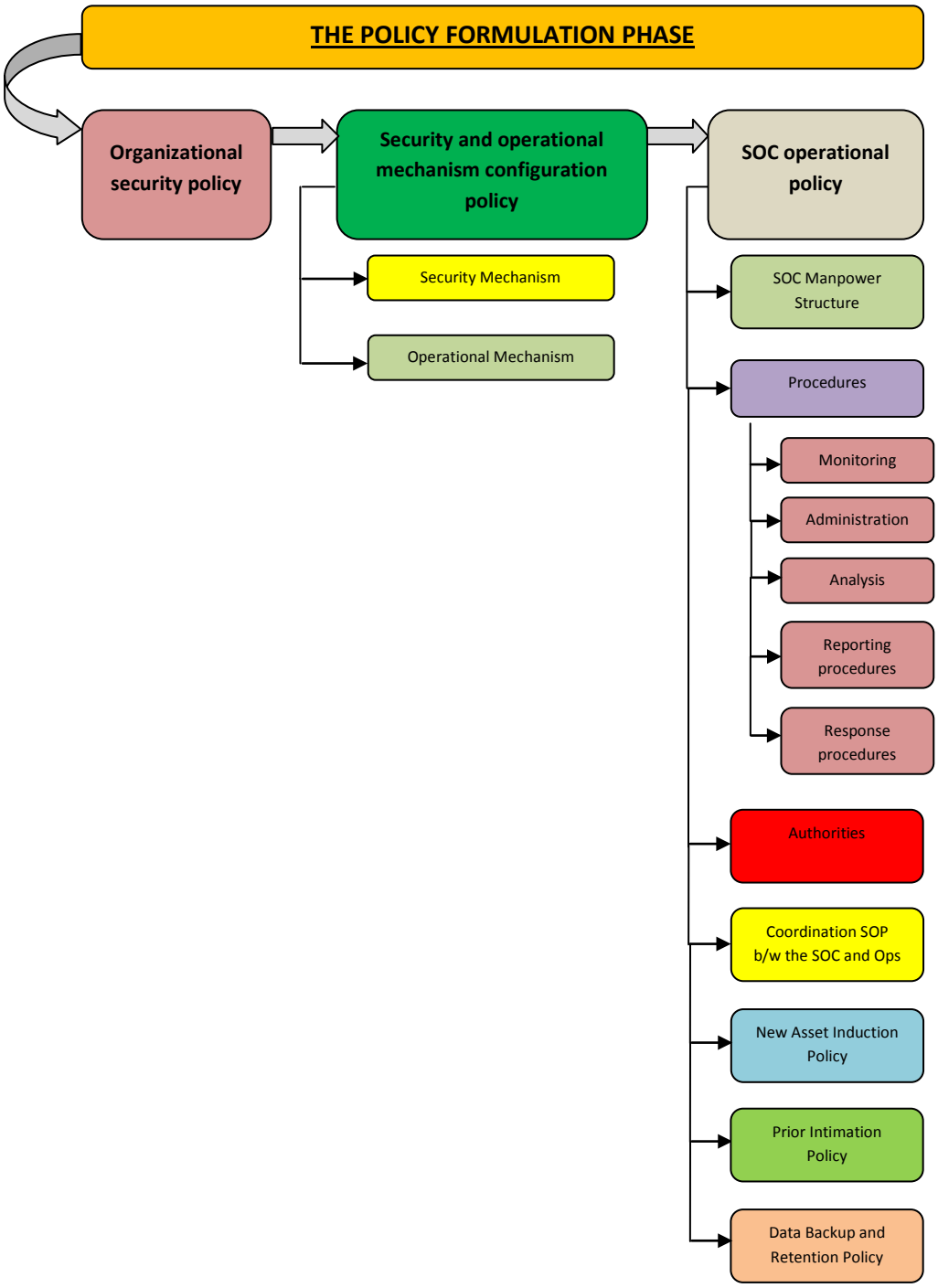

Fig 17. Policy Formulation Phase

7.2.4.1 **Policies**

Implementing security in an organization and then establishing systems to monitor that security are the two tasks which require a lot of coordination and sequential synchronization. This co-ordination can only be achieved if there are well defined and well thought of policies that provide a detailed guideline on what is expected out of the systems. Following policies are required at minimum within an organization

1) Organizational Security Policy. If we say this policy is that one piece of information, which is most vital to the complete project of security deployment and monitoring, it would still be an understatement. Basing on the already evaluated threat scenario and the organizational requirements of confidentiality, integrity availability, this policy answers the following questions

- Differentiates what all is allowed and what is not allowed. This differentiation is done from two perspectives
  - The end user
  - The administrator (domain wise).
- The policy unambiguously states as to what all needs to be stopped.

2) Security and Operational Mechanism Configuration Policy. This policy is based on the organizational security policy, decided previously. It specifies the standard configuration scenarios for the following entities

- Security mechanisms
- Operational mechanisms

The policy is supposed to define standard baseline configurations which should be met for every security and operational mechanism according to its employment. It should specify

- What all needs to be configured at minimum.
- What all needs to be stopped.
- Which configurations are undesirable?

3) SOC (Security operations Center) Operational Policy. This policy is a guideline on how the security operations centre would be run and maintained. It should be a combination of sub policies on the following aspects:

a) SOC Manpower Structure. Right before the actual deployment of SOC, its manpower structure that would be required to deploy and monitor it should be streamlined. This task is registered in a written form through this sub policy.

b) Procedures. The various procedures required to run a SOC can be divided into six main categories as follows:

i. **Monitoring.** This sub procedure streamlines the finer points of monitoring activity that would be carried out in SOC. It elaborates on the following:
   - Who all will monitor
   - How will they perform their duties
   - SOPs during performance of duties
   - SOPs for change of duties

ii. **Administration**. This sub procedure describes the following:
   - Who all will administer SOC
   - How will they perform their duties
   - Their responsibilities
   - Tasks and co ordination with operations teams of the organization

iii. **Analysis.** The procedure for analysts will be described in this sub section addressing the following:
   - Who all will be analysts?
   - How will they perform their tasks?
   - Their responsibilities.

iv. **Reporting procedures**. How would events, incidents and offences be reported and what would be the chain of authorities to which they would be informed. This sub procedure should contain the following two sections:
   - Reporting mechanism
   - Flow of information

v. **Response procedures**. This sub section contains the details of the response methodology that would be followed in case an offence or violation occurs. It describes the mechanism and people involved in the

response, their flow of information as well as the flow of orders and their corresponding levels. This procedure should be dealt with in following sections:

- Response mechanism
- Flow of information
- Flow of orders

c) <u>Authorities.</u> In order to run a coordinated and synchronized SOC, which has clarity of objective and vision, it is very important to define authorities of people. It consists or demarking the jurisdiction of people involved in the running, maintenance and approval process of SOC. This section should be based on following salients:

- Specify the appointment holders responsible for the operations or decision making of SOC.
- Who can order what?
- Decide the authority parameters for each entity.

d) <u>Coordination SOP between the SOC and Ops Team at Central and DC level.</u>

One of the major problems faced in the smooth functioning of SOC is the non synchronization between the SOC team and operational authorities at the central or remote locations. In case of an event, offence or violation the SOC team needs to contact several authorities in the IT architectures administration to get the mitigation process executed. This unnecessary bureaucratic red tape creates a non synchronous environment and introduces undesired delays in incident response. In order to address this problem a detailed SOP needs to be streamlined as part of the overall SOC operational policy, which not only earmarks contact persons at the central facility as well as in every DC for SOC, but also elaborates as to which administrator will perform what job in case assistance is requested from SOC and vice versa.

e) <u>Policy – New assets induction/ installation</u>. Prior to the induction of any new asset in the architecture, it will be inspected, analyzed for threat vectors, checked for compatibility with SIEM, and a comprehensive certificate in this respect be rendered by SOC team. The asset will be configured and made to report to SOC simultaneously while being inducted.

f) Prior Intimation Policy. This sub policy is suggested in order to keep the SOC team on board whenever any administrative, operational or configuration activity takes place at the data centers. During the survey conducted, it was observed in most organizations, that whenever the administrators were carrying out an activity at their end, the SOC team had no knowledge of it. This resulted in a huge number of events being generated at the SOC screens and triggered the investigative processes at SOC. After much effort the events were found to be false positives since the administrators were carrying out some operational activity at their end. This gave rise to the need to introduce such an SOP as part of the overall SOC operational policy, which binds the administrators to officially inform the SOC team about any significant maintenance or configuration activities carried out at their end. Following scenarios are quoted as examples for the readers.

i. Carrying out routine maintenance – patch management
ii. Upgrade of infrastructure including networks, O/S, applications servers, storage, DB e.t.c
iii. Creation of new administrators/ power user usernames passwords.

In actual there could be many more situations which need to be brainstormed exhaustively while formulating this sub policy.

g) SOC Backup and Retention Policy. The organization needs to decide, prior to the deployment of the system, the period for which it will retain the events' data. The policy will also specify how data backup will be made and where it would be retained. In addition it would also contain the complete procedure of how it would be recovered in time of need.

7.2.5 The Deployment Phase

The deployment phase deals with the actual deployment process of SOC with a primary focus on the SIEM solution. The subject process is divided into five sub phases which are carried out after the completion of preliminary spade work described in the succeeding paragraphs. An over view of deployment phase is as follows:

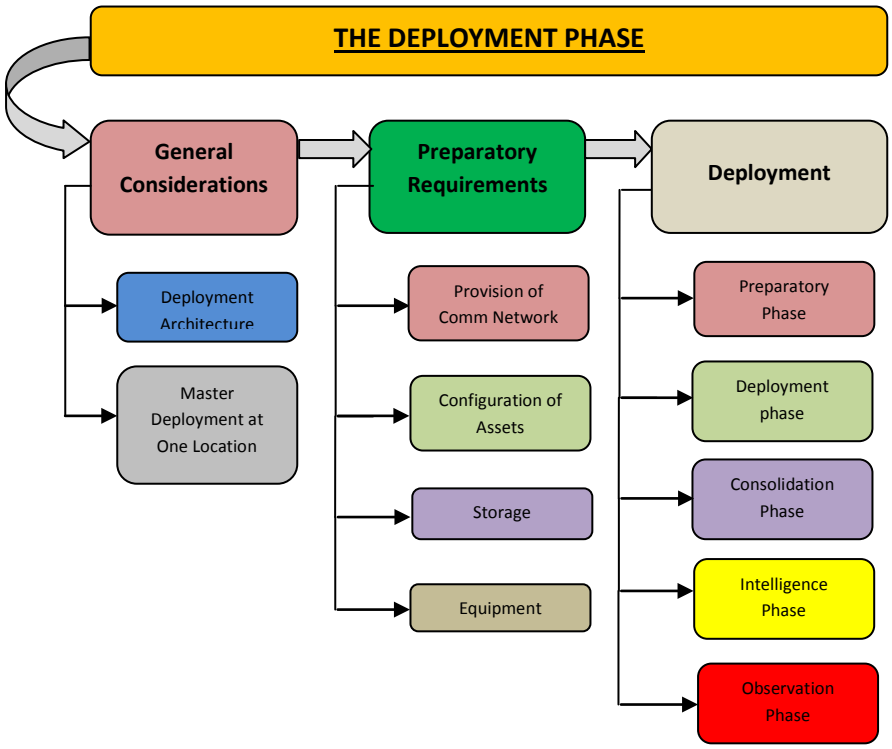

Fig 18. The Deployment Phase

7.2.5.1 General Considerations

1) Deployment Architecture. There could be various methodologies to deploy a SIEM solution. The methodology chosen depends on fol things

- The overall network architecture of the organization across the country.
- The bandwidth available between the sites.
- The processing power available at the central location and remote sites.
- The maximum capacity of information and events that one SIEM instance can handle.

Basing on the above mentioned considerations the deployment can be of two types:

a) **Central**: All SIEM components, deployed centrally for the complete country with information and events from all across the country flowing directly to the central SIEM.

b) **Distributed**: A standalone instance of SIEM deployed for each Data Centre. This instance is to carry out all tasks of collection, co-relation, offence generation on its own and for its own Area of Operations. However in such a system, a central SIEM would be installed at the central location. All individual SIEMs would be synchronized with this central deployment to forward only their offences (not events) to its location. In distributed deployment the central location will have a master SIEM with the interfaces of all subordinate SIEMs visible through remote access for any further forensics/ investigation.

c) **Deployment Architecture Suitable for Closed IT Organizations**. Keeping in mind the extensive network infrastructure of Closed IT Organization, and the available bandwidth between the remote and central sites, the only suitable option is that of distributed deployment.

2) **Master Deployment at One Location**. Keeping in mind the criticality and importance of SIEM systems in successful operations and effective implementation of SOC it is desirable that the SIEM solution be deployed and optimized at one data centre first. This deployment should be carried out with an aim to be a model installation, with the SIEM being configured for all possible imaginable scenarios, exploiting its potential to the maximum. All fine tuning, infusion of intelligence and rule formulation according to the policies of the organization should be carried out in this deployment.

An extensive penetration test on this Data Centre should be carried out after the completion of deployment to verify whether the system meets its stated base objectives or does it need further fine tuning.

Once it is complete this should be declared as the master deployment and should be a base guide for all next deployment. All next deployments should be made a replica of this, provided the architecture and flow of other sites/ Data Centers is the same as that of this. If small differences do exist in the infrastructure of next Data Centers, the same deployment should be tweaked for any minor changes.

7.2.5.2 Preparatory Requirements for Deployment

1) Provision of Communication Network. A dedicated IP subnet, for SOC, should be earmarked which should preferably belong to the backend pool. Each asset should be able to communicate with the SOC net prior to deployment.

2) Configuration of Assets. Every asset needs to be configured so as to report its events to SIEM. This configuration could either be done by pushing an agent on the asset or configuring the asset itself. Whatever is feasible should be technically decided by the SOC design team. This step should be carried out after the basic SIEM servers have been established and their internal configuration completed.

3) Storage. A robust and dependable SIEM solution must have a dedicated storage. This storage could be in the form of a dedicated share on SAN.

A very important aspect is to define a clear and concise policy for the period of retaining events. As a thumb rule, the maximum amount of time for which an event can cause adverse effects to the system, becomes the retention period of the event.

4) Equipment

a) Servers. Any SIEM system is required to process large amounts of data in real time and extract threat intelligence out of it. This requirement demands high capacity servers which can support such a demand with adequate processing power. Any compromise in this regard may not only effect the viability of the complete project but may also effect the operational efficiency of Security Operations Centre. Large capacity RAMs would be required to support the demanding nature of operations of SIEM.

b) High Availability. A SIEM system is so critical to the overall well being of the IT architecture that the organization cannot afford its unavailability. It acts as eyes and ears to the security experts who are watch guarding the IT domain for any pilferage/ breach/ violation. Therefore it is recommended that the system may always be deployed in high availability. Necessary equipment in this regard may be pre planned.

Moreover it should be ensured that high availability is implemented physically on two separate machines rather than in a virtual environment, in which two redundant machines run on one virtual platform.

c) Security Operations Centre Room. In order to establish a central nerve centre from where the complete organization across the country could be monitored, and

decisions regarding appropriate reactions and responses could be implemented, a Security Operations Centre facility is required to be built at the central location. Classically speaking this central SOC would comprise of following:

- Several large display screens (preferably video wall).
- Work desks for operators
- Work cabins for administrators with computer terminals.
- Offices for analysts with computer terminals.
- Communication equipment, i.e. telephone lines (preferably one at each desk) for prompt communication across the country, with data Centers.
- Off line processing machines (computers) for maintaining and downloading backups.
- Racks where backups can be stored for future use.

Similar equipment at a smaller scale would also be required for the regional SOCs established within Data Centers.

7.2.5.3 Deployment.

1) The Right Environment. The deployment of SIEM systems, for the establishment of SOC, is a major event in an organization. Since, after the establishment of SOC the usual freedom of administrators and the non observance of users would be greatly curbed, therefore it is a common sight in organizations that right at the establishment phase the project of SOC faces a lot of resistance, some announced some tacit.

The resistance may range from non co operation by Data center administrators to not providing the required access to the deployment team, not creating administrator username passwords at the management servers to not providing them the presence of administrators to work with. The two main reasons, for this non conducive attitude of administrators and organization's operations team, are:

- The misconception that SOC/SIEM is there to curb their legitimate working freedom.
- The feeling amongst Data Centre administrators that SOC has no utility for them. It is there as a reporting mechanism for the higher ups sitting at the center.

There are two ways in which any organization can counter the above mentioned attitude and ensure that the project is successfully installed and administered.

a) Make them the Stakeholders. It is the responsibility of the deployment team of SOC to take the Data Center administrators on board. They should explain the admin and operations team at each location that the system is not to catch them. It is there to assist them to catch bad people. And that they are a part of the overall security mechanism, not a victim of it.

b) The authorities desirous of getting Security Operations Centre implemented should give adequate authority to the deployment and admin team of SOC, so that they can dictate the organizations security policy to the under command sub organizations if the need arises and may get the overall vision implemented despite odds.

2) Phases. The complete deployment of SIEM solutions leading to the ultimate establishment of Security Operations Centre can be carried out in five phases

- Preparatory
- Deployment
- Consolidation
- Intelligence
- Observation

3) Preparatory Phase. In this phase the following is to be ensured:

a) The IP nets of all assets to communicate with SOC net.

b) Storage shares at SAN should be prepared and ready according to the required capacity and configuration.

c) Administrative accounts to be provided to the SOC deployment team on the management servers of the Data Centre. These accounts should be properly named and a log record of their activity be kept for future use.

d) Hardware equipment required for deployment of SIEM to be prepared by the Data Center administrators and placed in the rack locations before the arrival of the team so that time and efforts can be converged towards the actual tasks of configuring and making the SIEM intelligent.

4) The Deployment Phase

a) Establishment of SIEM Servers at the Facility.

i. The first action which the deployment team should take on reaching any Data Center is to establish the servers and install all the components of SIEM.

ii. After the installation the deployment team should maintain a document with itself, specifying the following information about the SIEM servers

- Make and type
- RAM capacity
- Location inside the server room
- Physical connectivity diagram with the rest of the Data Center i.e. what all connections are being made and with which devices through which ports.

iii. Moreover the team should also physically mark the SIEM servers in clear so that in future any activity in the server room may not accidentally affect the SIEM servers.

b) <u>Clearance of Network</u>.

i. After the establishment of SIEM servers, the depl team's next task is to ensure two way communication between the SIEM network and the rest of the assets in the Data center.

ii. **<u>Updated Asset List Required</u>**. In order to carry out this step effectively, it is vital for the depl team to have an updated asset list of the DC, mentioning all devices that are present in the facilities server room as well as its AOR. This may include all network devices, O/S, applications, databases, storage devices, upload PCs and any other item which forms part of the IT infrastructure. It should be ensured that no asset is missed out of the list at this stage. Incase such a lapse takes place it may have very far reaching implications on the security of the organization.

iii. Efforts should be made to ensure that the network connectivity established between the SIEM servers and data centre devices is permanent. No future tweaking of the network may effect this connectivity, as it may open a loophole for pilferage. Such efforts may consist of monitoring the firewall policy configured for SOC communication.

c) Integration of Storage for Event Retention. SIEM is a system which processes large quantities of events in real time and extracts threat intelligence. Resultantly it requires its dedicated storage space for retention and recall of events. This storage space can be in the form of dedicated hard disks installed within the servers or SAN shares earmarked for SIEM. Both the options have their drawbacks and benefits. Which one to chose depends on the overall architecture and storage requirement of the system.

As a thumb rule if the underlying network within a data centre which connects SAN to other devices is robust and can handle large information bursts, then the ideal choice is a dedicated share at SAN. Otherwise a separate large capacity hard disk would suffice. But then the capacity has to be carefully chosen based on the forecast of events that are expected to be encountered.

Earmarking the storage for the system does not end the job. Its integration with the system, so that the SIEM solution can throw and recover large events from it in real time, is the main impeding task. While carrying out this integration the following should be ensured:

i. The storage should preferably be mounted on the SIEM system rather than remote writing through IP network.
ii. Mechanism should be devised which brings the storage itself under effective monitoring of SIEM.

d) Integration of Devices

i. Network Devices. While integration network devices with SIEM for event reporting and threat monitoring, the following aspects are to be kept in mind

- Instead of collecting all events at SIEM and then sifting the useful ones from the garbage, the events to be collected should be sifted right at the source. Only those events should be configured to report to SIEM that are required for threat intelligence.
- Which events are required to report, this decision is to be based on two factors

  aa. The overall security policy of the organization.

  bb. The threat evaluation carried out in first segment.

- The devices should also be configured so as to throw their flows to SIEM for analysis.

ii. **Operating Systems and Applications**. All types of operating systems as well as custom made/ off the shelf applications that are being used in the architecture need to be configured to throw their logs to SIEM. The selection of which all logs to collect depends on the same two factors that were used for making decision in the network device integration.

There are two methods of configuring the operating system servers for log reporting. First is to configure the server's own log file to throw its events to the SIEM. Second is to install a SIEM agent on the server. Which option to select depends on the quantum of logs expected from the server and the availability of agents. If a high quantum of logs is expected then the agent option is better since it minimizes the load on the network by sifting the events right at the source and collecting only those that are direly required.

In case of applications they need to be configured to forward their logs to SIEM without an agent.

iii. **SAN integration**. The storage area network (SAN) is the device which actually houses all the data of the organization. It is a prime candidate for 24/7 monitoring, and even a small administrative command run on it should be under watch. All record of whosoever is accessing it should be maintained whether they be users or administrators. This security objective can only be satisfied by integrating SAN with SIEM for monitoring.

iv. **Database Integration**. The recent cases of pilferage in large enterprises such as TJX marshal and JP Morgan indicate that Database security was the most neglected part of these corporations.

By virtue of architecture, the database servers reside behind several layers of network and application devices. For this reason, they are erroneously presumed to be safe by the admin and security experts of the enterprise. However this is not the case. The database infrastructure needs as

much security as any other section of the architecture. A vital part of that security is monitoring the database.

There are two methods in vogue with which Databases can be monitored through SIEM. First is to switch on native logging at the database. It is presumed that by switching on native logging at the database, its operational performance will deteriorate. How much this is true in large organization's scenario needs to be found out by extensive testing on sandbox environment. Second is to install third party software that may collect the database logs and forward them to SIEM. Which option to choose actually depends on the funds available and the database architecture.

However, it is recommended that after testing option one extensively on a sandbox environment, if the results are within tolerance limits, this option is the most economical and viable.

v. **Print Monitoring**. In a paper free environment, where all information resides on electronic media, printing is the most convenient and least observed method which can cause pilferage of data. Therefore integrating the print servers of the organization with SIEM for threat intelligence and pilferage monitoring is very important.

Print servers should be configured to throw selected events to SIEM, only those which are required to fill in the complete picture of organization's security posture. The decision as to which events need to be reported is based on the same two factors that hold for network devices.

5) **Consolidation**. The consolidation phase of any SIEM solution requires that a further configuration of the system be carried out so that the collected events, data, related offences and threat intelligence be presented in a simple, understandable and practical way to the user of the system. This phase is not limited to but will include the following important steps:

a) **Configuring Network Hierarchy**. The system needs to be configured so it can recognize the hierarchy of network. How this is to be carried out technically will depend on the SIEM solution you are using, since each solution has a different method of recognizing the network. However this research paper has been written, with IBM Qradar in consideration therefore the technical method of configuration for our organization can be specified in a

separate technical manual (a document recommended to be written in the maintenance and administration phase).

b) Configuring Retention Policy. Basing on the retention policy of the organization, decided in the analysis phase, the system should now be configured to retain the events up till the time specified and for the group of events specified. After the expiry of the said time the system should purge these events itself to make place for newer evetns. But before this purging, the procedure for taking backups off line and storing them should be streamlined. This gives rise to the next logical step of consolidation

c) Configuring Backup Policy. The system basing on the backup policy decided in analysis phase is configured to take automatic backups. Those backups are then manually stored offline for future use. This activity to be regulated through SOP by including it in a maintenance checklist proposed in the maintenance phase.

6) Intelligence. Even the best of the SIEM solutions in the world cannot achieve their desired objectives if the intelligence part of their deployment is ignored. A SIEM solution, in its most basic form, is nothing but an event collector. A device which collects logs, events and flows from across the network architecture. It is the intelligence for which this system is tuned and configured, which gives it the cutting edge.

Infusing intelligence means only one thing, configuring the system to recognize all possible data breaches, violations of security and information pilferage attempts by scrutinizing the collected event data. In other words the SIEM solution is programmed in this phase to interpret human intent (i.e the intent of users, administrators or attackers).

SIEM solutions work on rules, against which they can compare the incoming data/events, to pronounce whether an offence has taken place or not. These rules are either pre-fed or can be custom made to suit the security policy of an organization.

In case of a closed organization like ours, which has an indigenously designed architecture, it is required that extensive rules (called used cases) should be created in the SIEM. These rules should be in line with the security policy of the organization, decided in the administrative phase, and they should preferably cover all attack vectors/ scenarios identified during the threat analysis carried out in phase 1.

Just to give the readers an idea of what all can be monitored and identified through these rules, a basic specimen of minimum desired rules is as follows

S No	Use Cases
	Windows
1	Multiple login Failures
2	Multiple sessions of single user
3	Windows Configuration/policy change
4	Escalation of privilleges
5	creation of new windows machine
6	creation of new admin acct
7	attempted denial of svc
8	Use of flash drive on servers
9	malicious software detection
10	acct login of sensitive appts after parade hours
11	Buffer overflow attack
12	A new svc instl on server
13	System rebooted multipl times in a given time
14	Print auditing
15	Clearing Logs
16	Creation of cmd prompt
17	Creation of rdp/mstsc
18.	A new software instl on server
19.	Running of an executable file
20.	Acct lockout and reactivate
	Networks
16	Illegal Eqpt att
17	Single IP with multiple MAC addresses (MAC SPOOFING)
18	Detect a new VPN connection
19	Use of internet
20	MAC flooding Attack
21	IP and Port Scans
22	DHCP Starvation attack
27	instl of new nw eqpt (SW and FW)
28	attempted denial of svc
29	IP address from outside DC NW
30	NW traffic from hosts at odd hours
	Sun Solaris
31	Admin access of solaris server
32	Admin acct creation at solaris server
33	Route addition at server
34	Route deletion at server
35	Config change
36	Denial of svc attack

37	instl of new solaris machine
38	System rebooted multipl times in a given time
	WebSphere
39	Admin access of linux server
40	Admin acct creation at Linux server
41	system rebooted multipl times in a given time
42	Route addition at server
43	Route deletion at server
44	Config change
45	Denial of svc attack
46	instl of new Linux machine
	SAN
47	Mega file transfer
48	illegal zdrive access

Table 11. Specimen Use Cases

7) Observation. The observation phase of deployment begins only after completion of the above mentioned phases. This phase comprises of observing the complete architecture of the Data Centre for at least 48 hours, and to look out for any adverse effects, that the subject deployment of SIEM solution has had, on the operational performance of the system. In other words this phase is there to verify whether the IT architecture is still performing its basic tasks after the deployment of SIEM. If not then what are the factors that have hindered the normal operations of the Data Centre, identifying and eliminating them is also a part of this phase.

The following minimum aspects of Data Centre functionality need to be observed in this phase.

- Operational performance of all applications being served by Data Center. Any complaint of unavailability or slowness should be investigated.
- The connections of DB listeners with Websphere.
- Active Directory
- SAN for slowness and unavailability
- Overall network performance for any ping loss within the DC or remote locations.

7.2.6 The Maintenance Phase. A well established and properly configured SIEM/ SOC will achieve its objectives only when it is continuously maintained through requisite human resource structure and strict standard operating procedures and policies. The aspects needed to be developed in the organization for maintaining SOC are not limited to but will include the following:

- Human resource structure to run SOC.
- Reporting mechanism/ procedure.
- Response mechanism/ procedure.
- Co-ordination policy of SOC and Operations Team
- Improvement/ feedback Mechanism.
- Training of SOC/ Data Center Resources.

7.2.6.1 Human Resource Structure. Any SOC/ SIEM facility needs to be manned and maintained with a specific human resource structure. These resources not only man the SOC stations for monitoring events across the complete architecture, 24/7, but a specific group amongst them also analyses the events to trace back sources of any developing threats and coordinates prompt responses to such attacks, through Data Centers. Furthermore a much superior group amongst them, who is in possession of top level expertise, utilizes the collected big data to carry out forensics and create user/ threat profiles.

1) Proposed Infrastructure. The human resource structure required for SOC/ SIEM can be divided into two sub sections as follows

- The Central SOC.
- Data Center team.

2) The Central SOC

a) The HR of central SOC can be divided into five basic teams, as per the suggested design of SOC at the beginning of chapter 7. The resources of these teams are further sub divided into three tiers, each tier representing the expertise level of the manpower. The complete SOC HR should be headed by a SOC manager.

b) The suggested team and tier distribution is as follows:

i. SIEM Team

- Operators: Tier 3
- Administrators: Tier 2

ii. CIRT Team

- Domain Specialists: Tier 1

iii. Forensic Team

- Analysts : Tier 1

iv. Pentest Team

- Ethical Hackers: Tier 1

v. Compliance Team

- Auditors: Tier 1

vi. SOC Manager

c) Operators (Tier3 -SIEM). Operators are the watch guards who man the SOC stations 24/7, observing the complete AOR of all the Data centers, on central screens, for anomalous events and offences. As soon as they observe any anomalous behavior in any data center they either carry out preliminary investigation themselves or report the matter to the administrators (tier 2). The day to day procedures, SOPs and reactions observed by these operators are guided by an extensive Operational SOP of SOC, which is developed keeping in mind the security policy of the organization.

d) Administrators (Tier 2-SIEM). Administrators should be a step superior to operators, both in appointment and as well as depth of knowledge. They are the experts, to whom events are reported in case they fall under the category of violation, pilferage or breach i.e. offences. The administrators carry out following duties

i. Study the reported offences in detail, carrying out preliminary investigation by going through all the available information from regional and central SIEM.
ii. During the process of investigation coordinate and inquire from the Data Centre teams at all levels, in order to establish the cause of the offence.
iii. In case an event requires physical mitigation, forward the offence to CIRT team and remain in their support for the mitigation of the subject event.

iv. Coordinate immediate response/ reaction with the Data center teams, through CIRT to mitigate the developing threat.

v. Carry out configurations and fine tuning of SIEM, deemed necessary as a result of practical scenarios or shortcomings communicated from supporting teams.

Keeping in view the sensitive and the prime nature of job of SOC administrators, it is highly recommended that the administrators should be placed directly under the command of the SOC Manager and further under the command of CEO. They along with the SOC manager should be given the privilege to report any incident directly to the highest most authority of the organization, through their administrator team lead, and take direct orders from him. Any bureaucratic channel in between the administrators, SOC manager and the highest decision making authority should be avoided, to promote in time reporting and quick and authoritative reactions to security incidents.

These administrators are like quick reaction forces which should be directly under the command of the general fighting the war.

e) **Analysts (Tier1 – Forensics)**. Analysts of SOC are analogous to the Sherlock Holmes of UK. They are the highly trained, skilled and well equipped investigators who, collect all the required evidence both from the SIEMs and on site, reach to the depth of any attack/ violation/ breach, ascertain the reasons and lapses which caused it to happen, and give valuable feedback in the form of a formal report which either inducts a change in the operational policy or triggers critical amendments to the existing procedures and SOPs. They are specialists who are invoked for special purposes.

Moreover, basing on the chornoligical data available, these analysts maintain a threat profile and user posture, with an aim to predict any attack which is in the formulation stage. Thus their functionality is critical to counter the phenomenon of advanced persistent threats.

f) **Domain Experts (Tier 1- CIRT Team).** CIRT team domain experts are the first people contacted and made to react to an incident by the SIEM administrators. They are placed at tier-1 keepin g in mind their expertise and the required authority they are supposed to exert on the operational administrators. Their job description requires them to have a fair

knowledge of the Data centre working and its flow architecture. For this reason it is preferable to have domain specialists in this team, who have served for at least three years as domain administrators in the operations of any Data Centre. Suggested duties and mandate of the CIRT team are as follows:

i. In case an offence is reported, immediately coordinate with the central Data Centre Operations team or remote Data Centre operations team and resolve or mitigate the issue.

ii. Guide and instruct the data center teams to carry out specific actions and administrative/ operational procedures in order to ensure that the incident does not take place again.

g) **Ethical Hackers (Tier 1: Pentest Team)**.The basic duty of pentest team resources is to keep probing the complete IT architecture proactively for loopholes and pilferage scenarios, and then report the matter to SOC manager. Moreover they provide vital breach information and overlook the improvement in SOC due to changing threat scenarios.

h) **Auditors (Tier1: Complaince and Audit team)**. As the name suggests these are the people who check whether the IT organization and its sub organizations are complying to pre decided policies or not. Moreover they also carry out vulnerability scans of the architecture at regular intervals and update the chain of command about the results.

3) **The Data Center Teams**. Each data Center should have a team comprising of at least four members. This team is to carry out following generic duties:

- Man the regional SOC station 24/7, dividing the duties amongst themselves as is administratively feasible.
- Observe and report any unusual activity that takes place in their AOR, to their command as well as central SOC directly.
- Respond to incidents on orders from the central SOC and assist the central SOC authorities in investigating and mitigating threats on ground.

a) The Data Center team can be divided into two groups:

i. **The Operators Group**: Four members who man SOC stations and report offences, coordinate responses and receive orders from the central SOC authorities.

ii. **The Response Team** : May comprise of the existing administrators of the Data Center who are required to physically react to any reported incident and mitigate the threat on ground.

iii. **The ISO**. The executive head of any Data Centre is supposed to act as the Information Security Officer also. This appointment is mostly ceremonial and is kept for situations where clarity of orders or resolution of conflicts between the team members is required.

4) Diagrammatic Representation.

A diagrammatic representation of the HR structure of SOC is as follows:

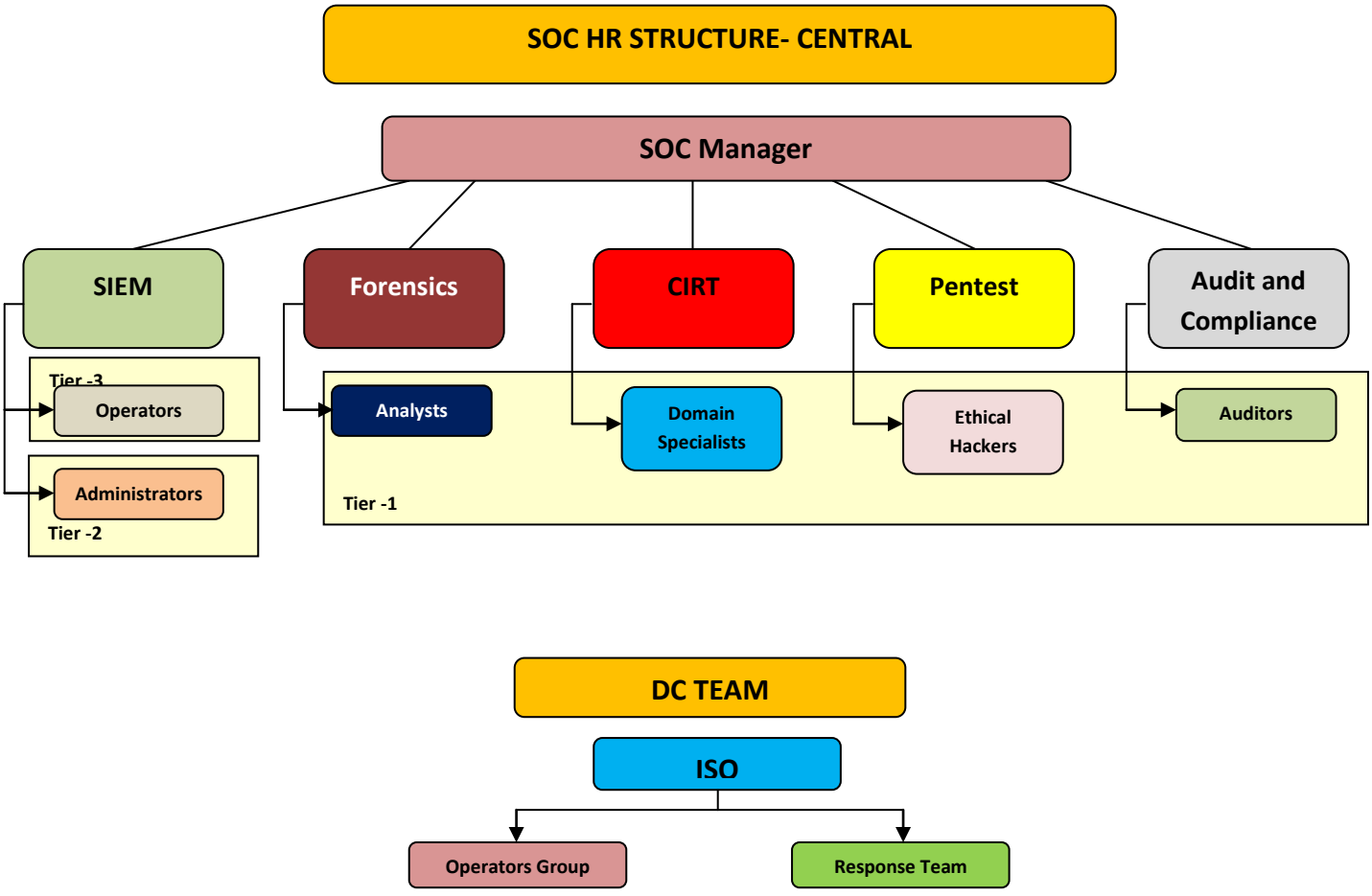

Fig 19. SOC HR Structure

7.2.6.2 Reporting and Response Mechanism. A vital procedure which is very necessary for the smooth functioning of any SOC/ SIEM system is the reporting and response mechanism. Although they are two distinct entities but they are designed and carried out simultaneously to ensure coordination of effort. The formulation and contents of these mechanisms may vary according to the operational environment of each organization but the policy governing them should satisfy the following general guidelines.

1) Reporting Mechanism.

a) It should clearly state which all types of events would be mitigated at regional level with information to the central SOC and which will be forwarded to central authority for guidance/ orders.

b) It should streamline the path of flow of information and the path of orders.

c) It should unambiguously define the format of reporting incidents and receiving orders and the channels through which they would be received.

2) Response Mechansim

a) This part of the policy should contain an exhaustive list of scenarios of events, incidents or offences.

b) It should clearly specify which member of the SOC infrastructure will act how in each particular scenario.

c) Given the intelligent nature of attacks and violations, the scenarios could be never ending. It is advisable that broad but exhaustive classes of scenarios should be made.

3) Diagrammatic Representation. A diagrammatic representation of the reporting and response procedure, combined along with their information flow is as follows:

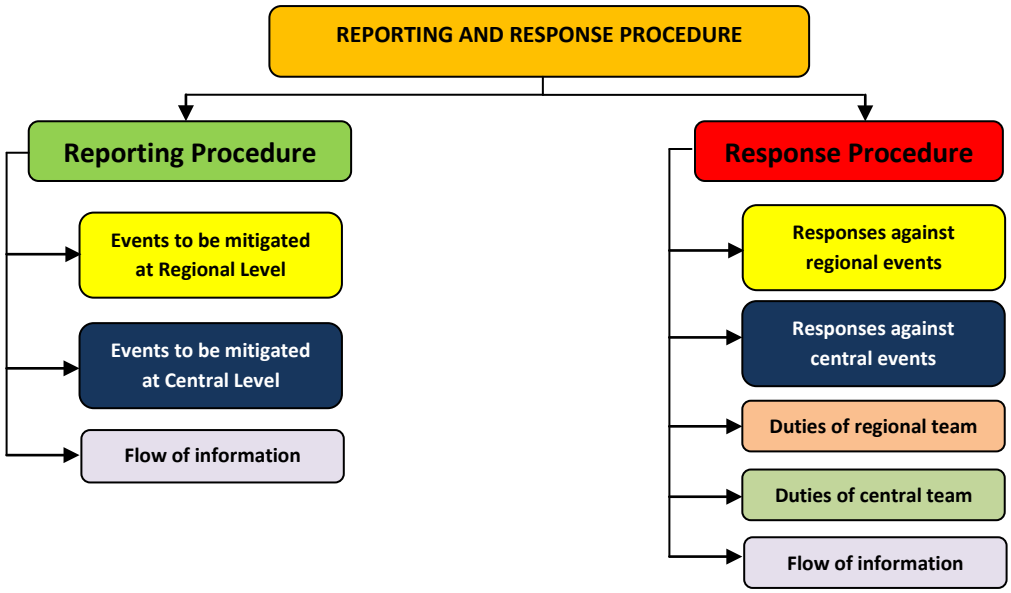

Fig 20. Reporting and Response Procedure

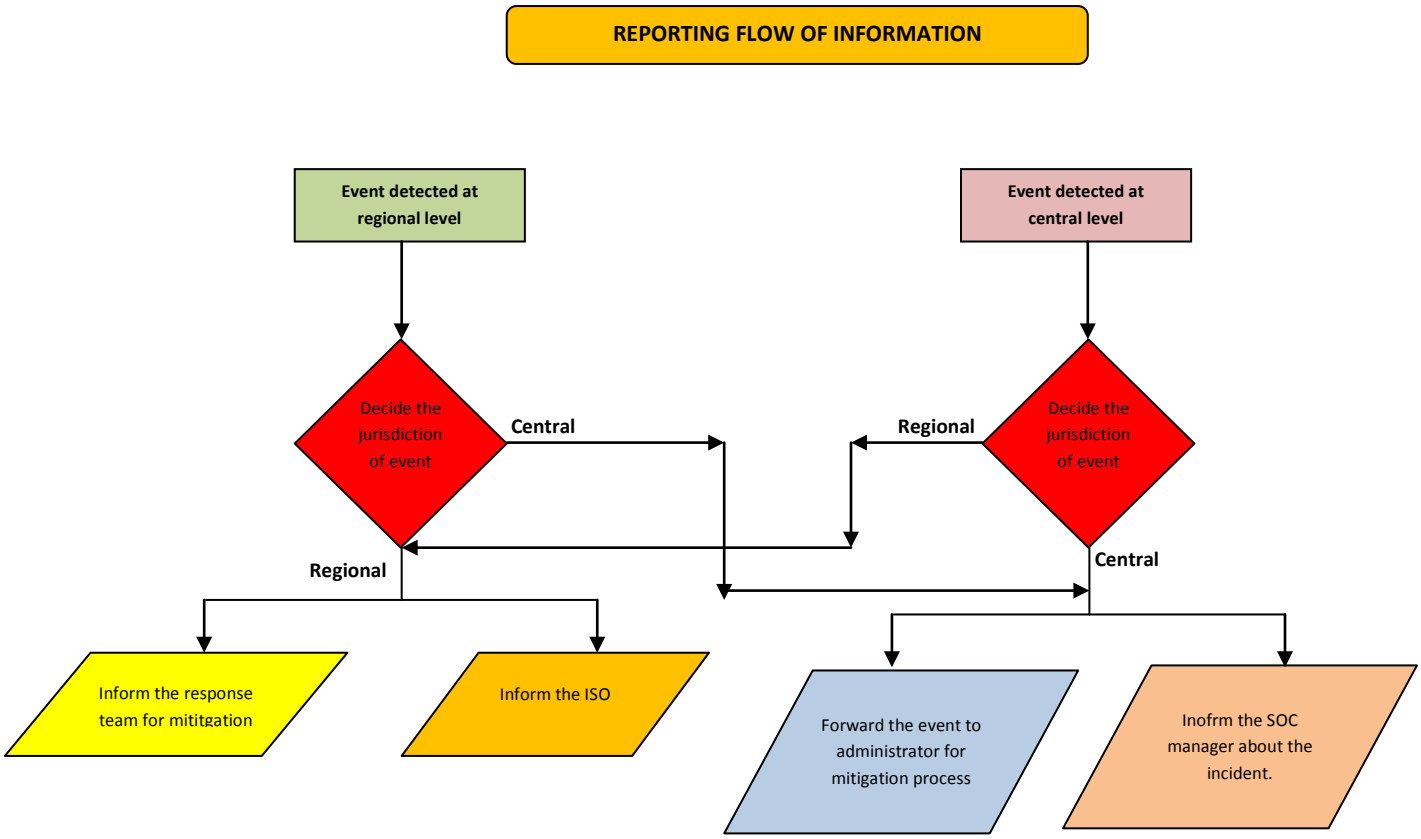

Fig 21. Reporting Procedure Flow

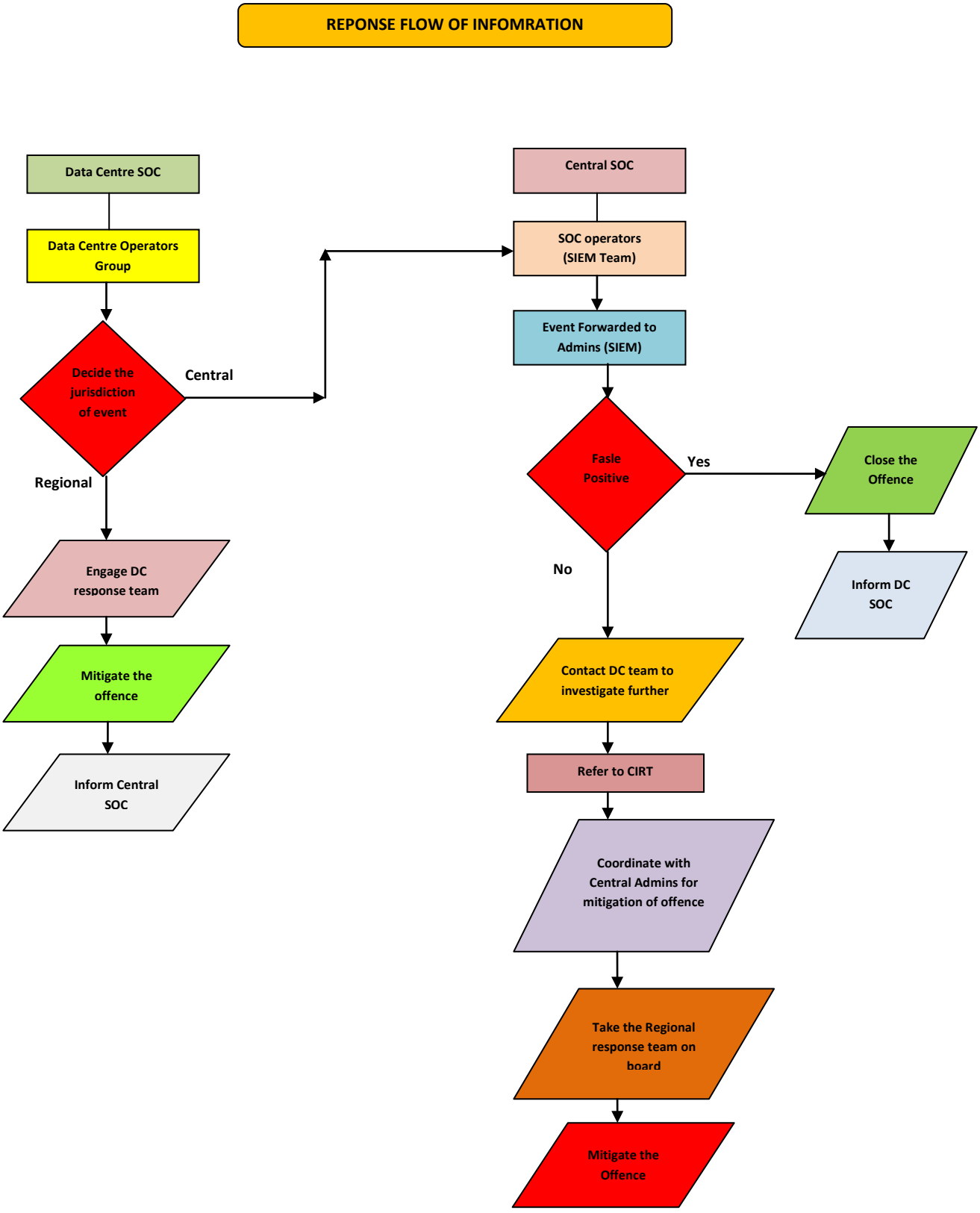

Fig 22. Response Procedure Flow

7.2.6.3 Co-ordination between SOC and Operations. In most organizations around the world a common problem which is faced by SOC teams is that the regional/ central operations teams, whenever carrying out their routine maintenance tasks or upgrading or installing new assets within the infrastructure do not bother to either keep the SOC authorities informed nor do take them on board.

SOC teams which are continuously monitoring the infrastructure start getting events which appear as offences and a tedious and lengthy procedure of investigation is triggered which ends up in the events being found false positives. This not only wastes a lot of time but severely affects the operational efficiency of SOC/ SIEM.

Keeping the above in view a stringent policy should be devised having the following salients:

1) It should instruct in clear unambiguous terms all operations and maintenance teams to keep SOC authorities informed about any activity in the system.

2) All new assets which are to be inducted into the infrastructure should be vetted and reported to SOC for analysis first, so that SOC authorities can determine methods to integrate them with SIEM systems.

3) Any new administrator names should be created after informing SOC authorities in written.

7.2.6.4 Improvement and Feedback Mechanism. The SIEM/ SOC system also requires constant feedback and update from the users (data center administrators) for its improvement and enhancement.

It could be very much possible that altogether newer scenarios of threat and pilferage, different from the ones brainstormed before installation of the systems, can be encountered when the SIEM system goes into production. In order to keep the deployed SIEM system alive and self correcting/ improving, it is vital to have a feedback mechanism in place, through which anyone who is related to the operations of SIEM/ SOC can provide his end of the feedback to the concerned authority, which may include anything from the on ground problems of training and operations faced by the Data Center resources to even newly imagined scenarios of pilferage which need to be monitored.

Maximum effort must be exerted to make this feedback system as effective and vibrant as possible and it should not just be an eye wash.

1) <u>Categorization of Feedback</u>. Feedbacks can be broadly categorized into three types as shown in the following figure

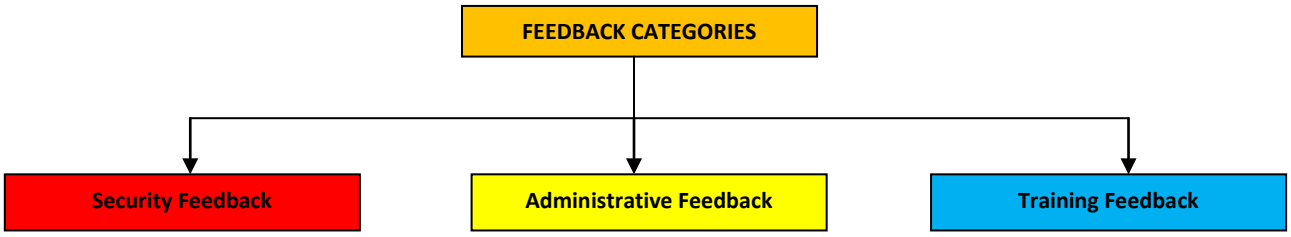

Fig 23. Categorization of Feedback

2) <u>Flow of Feedback Mechanism</u>. The suggested flow of feedback mechanism is as follows

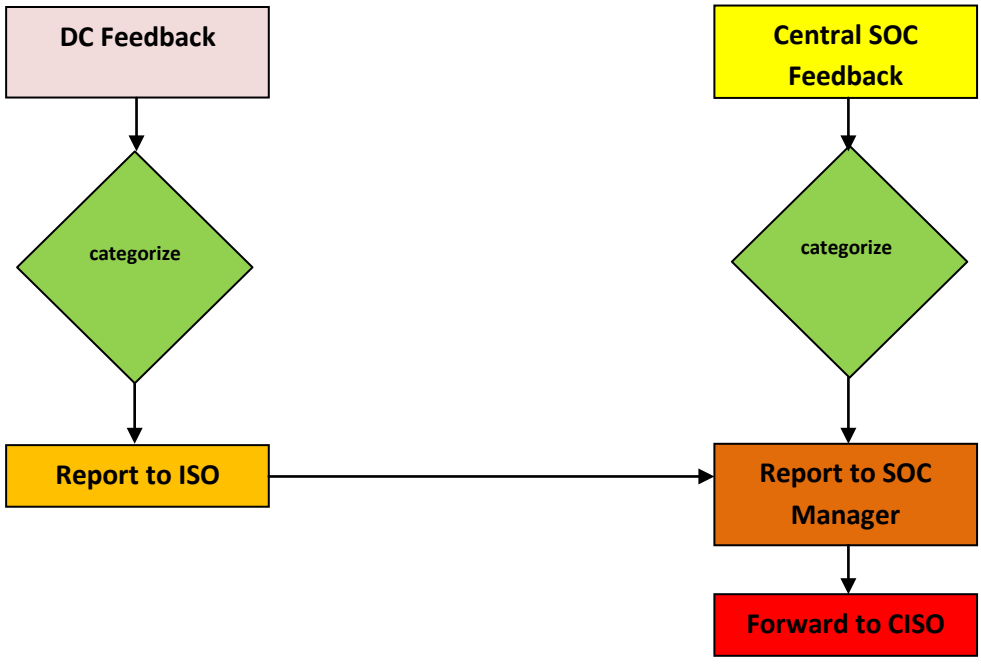

Fig 24. Flow of Feedback

7.2.6.5 <u>Training of Resources</u>. Improvement and enhancement of SOC/ SIEM is a continuous and ongoing process, which can never be termed as complete. However a minimum threshold of expertise and smoothness in its processes can be obtained by aggressively training the manpower handling it.

The training of manpower will differ according to the level/ appointment of resources however a general guideline, as per each tier, is appended as follows as to what all aspects the resources, handling SOC, need to be trained in.

1) **<u>For tier 3 (Operators)</u>**:

a) The general concept and implementation of SIEM solutions.

b) Working Knowledge of Organization's network architecture

c) Architecture of the flow of data within the Organization and its IT infrastructure.

d) Reading logs and events from different devices (network, O/S, servers applications, storage, DB)

e) Various types of attacks and their footprints.

2) **<u>For tier 2 (Administrators):</u>**

a) In depth knowledge of

i. Company's network.

ii. Company's data flow.

iii. Applications and OS used.

b) Updated knowledge on

i. Vulnerabilities of own architecture.

ii. Vulnerabilities of OS and applications (general).

c) Knowledge about attacks

i. Attack development patterns.

ii. How attacker thinks.

iii. Log generation pattern in case of attacks.

iv. Mitigation techniques of attacks.

3) For Tier 1:

a) Analysts (Forensic Team). Resources in tier 1 forensic team should be certified forensic analysts.

b) Domain Specialists (CIRT Team). Resources should have a secondary level certification in their respective domain, such as networks, windows, Database or SAN as well as minimum three years experience of serving in a Data Center.

c) Ethical Hackers (Pentest Team). Resources to preferably have following certifications

i. CEH (mandatory).
ii. Penetration Testing through Kali Linux (mandatory).
iii. Offensive security specialist (desirable).

4) For a particular tier, the skill sets of previous tiers are mandatory.

7.3 Summary. SOC and SIEM systems require extensive preparations and homework at the organizational level before they can be implemented in the most effective way. These pre-requisite steps provide the SOC/ SIEM their required cutting edge with which they can proactively monitor and safeguard the architecture. These steps when carried out in chronological order form a complete and all comprehensive methodology which provides an organization with effective reaction capability against IT threats, pilferages and violations.

Chapter 8

EVALUATION, RESULTS AND ANALYSIS

This section of thesis pertains to the evaluation of the proposed SOC framework against earmarked metrics or key performance indicators (KPIs). As a result of the survey conducted of several large IT Organizations, certain follies and shortcoming were highlighted within their SOC infrastructure and implementation. These loopholes along with other industry accepted performance metrics were combined to formulate a comprehensive list of KPIs against which the performance of proposed SOC architecture was evaluated. The aim of this evaluation was to ascertain the effectiveness of subject framework, its practical workability and how close it came to solving our given problem statement. For this purpose a small scale, hardware based replication of the actual IT architecture of closed organizations was created and data sets were obtained from it, before and after the implementation of the proposed framework on this test bed.

This provided us with a sound basis to carry out the final analysis and pronounce whether the suggested SOC framework is effective or not.

8.1 The Shortcoming in Existing SOC Implementations.

The survey of large IT organizations, revealed certain shortcomings and loopholes in their SOC infrastructure, which are summarized as follows:

Ser	Shortcoming	Description	Remakrs
General			
1.	Improper selection of security measures	a. A feature which was not present in the architecture was being mitigated b. Moreover a feature which had to be mitigated was not being look after c. Going after brand names: (1) No proper method of evaluating requirements (2) Brands were considered the best solution	

2.	Wrong placement of security measures	a. **Reason:** Improper or no threat evaluation and asset mapping b. **Effect on SOC**: Increase in false negatives and false positives	
3.	Configuration of security mechanisms not commensurating with the overall security policy	a. **Reason:** No security policy existed or no linkage to the policy established while implementing SOC. b. **Effects on SOC**: Soc was not able to catch events according to the desired security results	
4.	Improper Selection of SIEM Tool	**a. Reason:** (1) The selected SIEM does not support complete infra. Black holes left in security monitoring. (2) Solution not flexible enough (3) Brand names were sought instead of specific requirements. (4) No specific evaluation criteria for tools was followed.	
5.	Unplanned Human Resource induction	a. Somewhere less number of people and somewhere more than what was required, were employed b. Duties were not explicitly defined c. **Reason:** No human resource structure policy and training doctrine existed. d. **Effects on SOC:** SOC became a firefighting machine rather than a systematic security measure.	

Policies			
6.	No organizational security requirements spelled out	a. SOC was implemented with the sole aim of monitoring. b. **Reason:** Firefighting mode was adopted rather than following a systematic approach. c. **Effects on SOC**: SOC did not fulfill the desired objectives	
7.	No Security and Operational configuration policy	a. No standard baseline configurations defined. b. **Effects on SOC**: The job of SOC intelligence became more difficult. SOC works by grouping and categorizing events as offences. Every location had a different configuration not conforming to a central requirement policy. SOC treated every case as separate and was not able to form correlation. Resulted in an increase in false positives and decrease in sensitivity.	
8.	No SOC operational policy	a. New assets inducted were not compatible with SOC. b. No intimation to SOC was furnished before operations. c. **Effects on SOC**: Promoted wastage of efforts, increase in false positives.	
Deployment			
Preparation			
9.	Configuration of assets done incorrectly	a. **Reason:** No SOC and operational mechanism configuration policy existed. b. Resulted in agent less installation – choking	

		of bandwidth.	
10.	Storage and event retention requirements not streamlined	a. **Effects on SOC**: Insufficient storage, dropping of events, crashing of SIEM tool.	
11.	Comprehensive SOC infrastructure not present	a. **Reason:** No standard guideline or framework was followed to implement SOC. b. Effects on SOC: SOC was not able to provide desired results to its implementers and owners.	
Deployment			
12.	Resistance experienced from operations and administration teams	a. The operations and administration team of the IT organization resisted the implementation and proper functioning of SOC b. Reason: Right environment was not created. Admins were not made stakeholders. c. Effect on SOC: there was a disharmony amongst SOC and operations which adversely affected SOC's performance.	
13.	SOC servers not prepared with administrator's help	a. **Reason:** SOC authorities had no trust in the operations team. The administrators were not made stake holders. b. **Effects:** Problems encountered after deployment, adversely affected SOC, with no help extended from the administrators. Crated chances of SOC bogging down right during installation or not being deployed up to the mark.	

14.	No updated asset list demanded by SOC team, before deployment	a. Resulted in black holes left in security.	
15.	Storage and Database not integrated for monitoring	a. Storage and data base were not monitored for security scenarios. b. Resulted in the most important aspects of security being ignored.	
Integration			
16.	All events sent to SOC, no filtering or streamlining of events at source. No differentiation of which events are required to be reported	a. The urge to collect every event at SOC in hope of not missing out an event caused this phenomenon. b. This overburdened the SIEM tool as well as the SOC manpower unnecessarily. c. Resulted in increase in false positives and missing out of concerned offences by SOC operators.	
17.	No monitoring of DB and print logs	a. DB and print logs were not being monitored. b. An important part of security was missed out. c. **Reason**: No existence of comprehensive organizational security requirements.	
18.	Lacking baseline of desired intelligence from SOC	a. No baseline of desired information from SOC was defined. b. No customized rules for own architecture were made. c. SOC/ SIEM was installed and operated on default rules. d. Whatever rules creaeted were not in line with the overall security policy if one existed.	

Observation			
19.	Insufficient time for observation of IT architecture for stability after deploying SOC	a. The urge to get immediate results right after the switching on of SOC led to insufficient time being allotted for observing the IT architecture for stability. b. Resulted in the operational performance of IT architecture being affected.	
<u>Maintenance</u>			
20.	a. Human resource infra in place but no flow of information or reporting mechanism	a. **Effects on SOC**: Important information about events and offences got lost due to hearsay.	
21.	No separation of duties	a. The operators were performing as analysts also. b. This overburden the manpower. c. Effects on SOC: Manpower started sampling the offences. Important information was missed.	
Response Mechanism			
22.	No clear/ exhaustive list of events/ offences and their responses defined	a. Events were treated on incoming basis. b. Responses were completely left to human judgment c. Resulted in non standard methods of mitigating offences. Every time a new technique was adopted which caused undesired configuration changes in the operational environment.	
23.	No co-ordination between SOC and operations team	a. No coordination SOP existed between SOC and operational teams of the Data Centre.	

24.	No feedback mechanism from the end user	a. No feedback mechanism was employed through which shortcomings of SOC could be communicated by the end users and administrators to concerned authorities. b. Resulted in SOC becoming outdated and out of line with the current operational requirements.	
Training of Manpower			
25.	Training of manpower not streamlined	a. Resources were being employed on ad hoc basis with little previous knowledge of SOC operations. b. No growth or development of human resource capability was carried out. c. Effects: SOC was not operated at the desired professional mark.	
26.	No progress path for human resource development defined. No tier based knowledge requirements identified.	a. No criteria for evaluating the performance of SOC resources were developed. b. Resultantly no progress path was formulated, passing through which the SOC resources could get promoted within their hierarchy. c. Reason: No defined HR structure for running SOC existed.	

Table 12. Shortcomings in SOC Infrastructure of IT Organizations

8.2 The Methodology of Evaluation

In order to evaluate the proposed SOC framework, a hardware based test bed was created, which replicated, as nearly as possible, the IT architecture generally used in closed IT organizations. The test bed design has been explained in chapter 6, section 6.3, figure 12. It consisted of a windows, linux, solaris, application and DB server which were installed on the virtual platform of VMware. Moreover a hardware firewall and a switch were connected to the network. As a sample, five laptops with customized user applications installed were used to replicate the user base. Data sets were collected from the test bed, before and after the implementation of the framework features, and the results compared graphically to ascertain the efficiency and usefulness of the proposed solution. The KPIs used as well as their corresponding results are discussed in the succeeding sections.

8.3 Performance Evaluation Metrics

To gauge the performance of suggested solution, two kinds of metrics or KPIs were devised, namely quantitative and qualitative. For quantitative KPIs, tangible data sets were obtained from the test bed using before and after methodology. For qualitative KPIs argumentative reasoning was used, along with relevant references to concerned sections of the proposed framework, to prove their fulfillment.

8.3.1 Quantitative KPIs

The key performance indicators used for quantitative analysis are summarized as under and the underlying logic behind them is explained in succeeding paragraphs.

Ser	KPI/ Metric	Formula	Maximum Good Performance Value	Maximum Bad Performance Value
1.	Attack detection accuracy	(true positives + true negatives)/ total packets	1	0

2.	False positive rate	False positives/ total packets	0	1
3.	False negative rate	False Negatives (attacks missed)/ total packets	0	1
4.	Computational Cost	Cost=(1-attack detect accuracy) +K(False positive rate) : where K=FP-FN	<1	>1
5.	Sensitivity	True positive/(true positive + false negative)	1	0
6.	Specificity	Specificity= true negative/(true negative + false positive)	1	0

Table 13. Quantitative KPIs [9][10]

The above mentioned quantitative KPIs are based on the confusion matrix shown as under:

Actual\ Detected as	Normal	Attack
Normal	TRUE NEGATIVE	FALSE POSITIVE
Attack	FALSE NEGATIVE	TRUE POSITIVE

Table 14. Confusion Matrix [9]

1) **Attack Detection Accuracy**. It is a measure of accuracy with which any IT solution detects attacks. It is a ratio of total true positives plus true negatives divided by the total number of packets. The maximum value is 1 which signifies good performance whereas the minimum value is 0 signifying bad performance.

2) **False Positive Rate**. It is the rate of detecting false positives in any system, and is comprised of a ratio of the false positives detected to the total number of packets. The maximum value is 1 which is bad and the minimum value is 0 which is good.

3) **False Negative Rate**. The rate with which any system declares the events as false negatives. It is the ratio of false negatives detected to the total number of packets. Maximum value is 1 which is bad and minimum value is 0 which is good.

4) **Computational Cost**. It is the cost of computation associated with any IT system. Its mean value is 1, i.e. the acceptable level. It is calculated by subtracting the attack detection accuracy from 1 and then adding the false positive rate in it. Before adding the false positive rate it is multiplied with a constant factor K, which is defined as the gap between false positives and false negatives. The formula is shown in table 12. Any factor which recedes the systems performance such as false positive rate is added to the mean value and any factor which enhances the performance of the system such as attack detection accuracy is subtracted from it. The overall result if less than one is termed as good, and if more than one is termed as bad.

5) **Sensitivity**. It is a measure of how sensitive a system is to detecting correct events. It is a ratio between the true positives and the sum of true positives plus false negatives. The maximum value is 1 which is good and the minimum value is 0 which is bad.

6) **Specificity**. It is a measure of how correctly a system detects non offensive events as normal. It is the ratio between true negatives and a sum of true negatives plus false positives. The maximum value is 1 which is good and the minimum value is 0 which is bad.

8.3.2 The Quantitative Data Set Collected

The data set collected in relation to the quantitative KPIs, from the test bed, is summarized as follows. Specific framework factors, mentioned in the data set and results were earmarked for quantitative evaluation and data was collected before implementing them on test bed and collected yet again after their implementation.

Quantitative KPIs (Metrics)	**Framework Factors**																					
	Asset Categorization and prioritization		Relevant Configuration of Security Mechanisms		Deployment Design		Specific log configuration		Config for proper integration with SIEM		Storage Sizing		Source Filtering		Deployment methodology		Network Hierarchy Configuration		Retention Period		Use Cases/ Rules	
	Not done	Done	Not done	Done	Centralized	Distributed	Not done	Done	Not done	Done	Not done	Done	Not done	Done	With Agent	W/O Agent	Not done	done	Shorter	Longer	Not sync to threat map	Sync to threat map
Attack Det Accu (0: bad 1:good)	0.3	0.7	0.3	0.6	0.4	0.5	0.3	0.7	0.3	0.5	0.3	0.4	0.3	0.6	0.4	0.3	0.3	0.5	0.4	0.3	0.3	0.8
False Positive Rate (1: bad 0: good)	0.8	0.5	0.8	0.4	0.7	0.5	0.8	0.5	0.7	0.5	0.6	0.6	0.8	0.4	0.4	0.4	0.8	0.5	0.5	0.6	0.8	0.3
False Negative Rate (1: bad 0: good)	0.7	0.3	0.7	0.4	0.6	0.4	0.7	0.3	0.6	0.5	0.5	0.5	0.7	0.4	0.5	0.5	0.7	0.5	0.6	0.6	0.7	0.3
Computational Cost (should be low) (cost >1 : bad cost <1: acceptable)	0.9	0.6	0.9	0.6	1.1	0.6	0.9	0.6	0.5	0.4	0.9	0.8	0.9	0.4	0.8	0.7	1	0.6	0.9	0.8	1.1	0.6
Sensitivity (1: good 0:bad)	0.3	0.5	0.3	0.6	0.4	0.7	0.3	0.5	0.3	0.5	0.3	0.3	0.3	0.7	0.5	0.3	0.3	0.5	0.4	0.5	0.3	0.7
Specificity (1:good 0:bad)	0.2	0.5	0.3	0.6	0.3	0.5	0.2	0.6	0.3	0.5	0.4	0.4	0.2	0.5	0.5	0.2	0.2	0.5	0.4	0.5	0.2	0.5

8.3.3 Results of Quantitative Evaluation

1) Asset Categorization and Prioritization

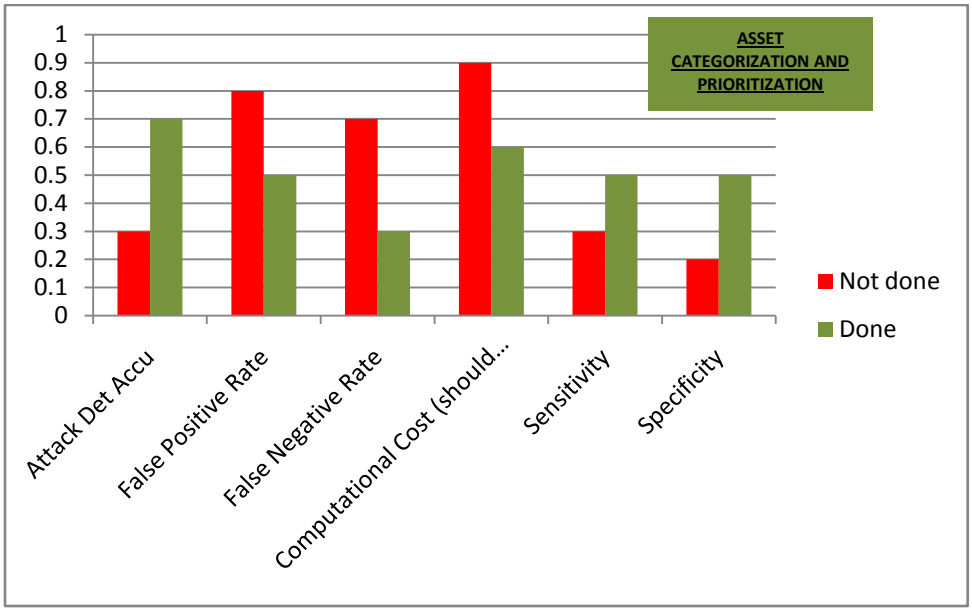

Fig 25. Results of Asset Categorization and Prioritization

2) Relevant configuration of Security Mechanism

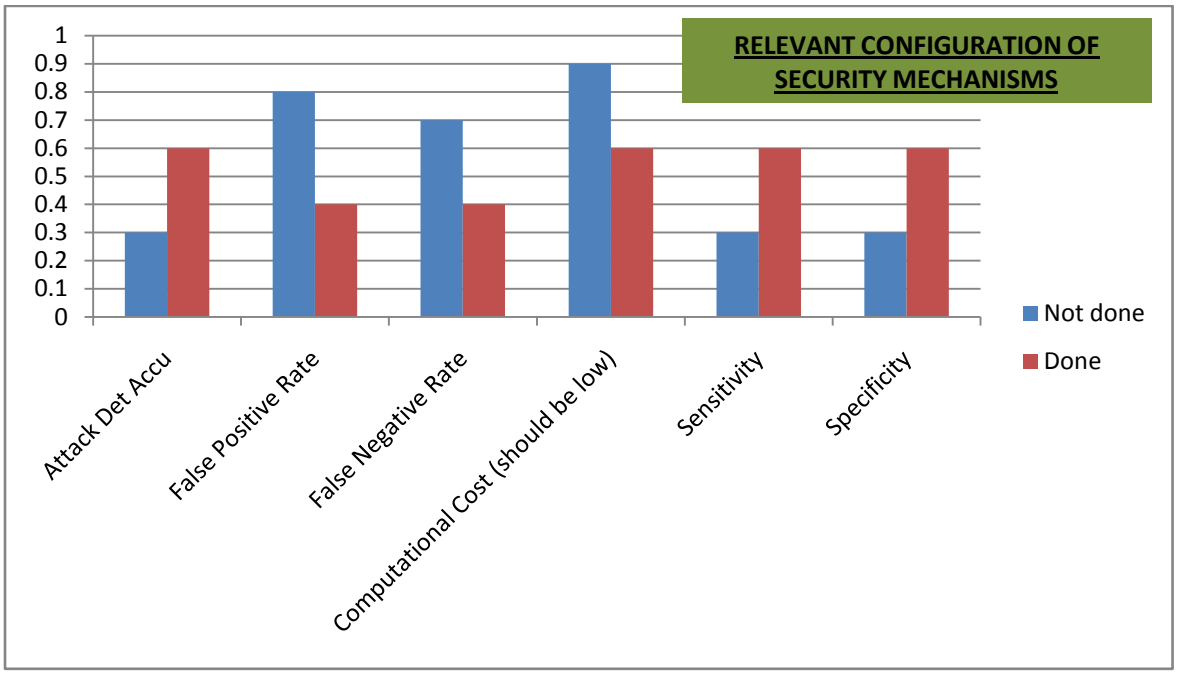

Fig 26. Results of Relevant Configuration of Security Mechanism

3) Deployment Design

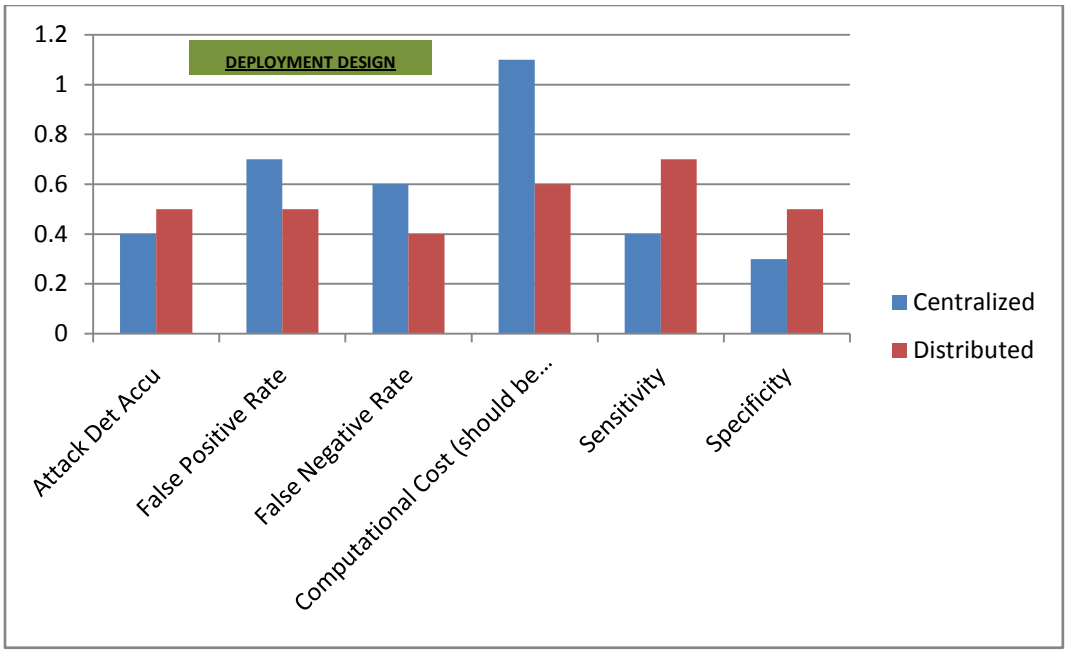

Fig 27. Results of Deployment Design Implementation

4) Specific Log configuration

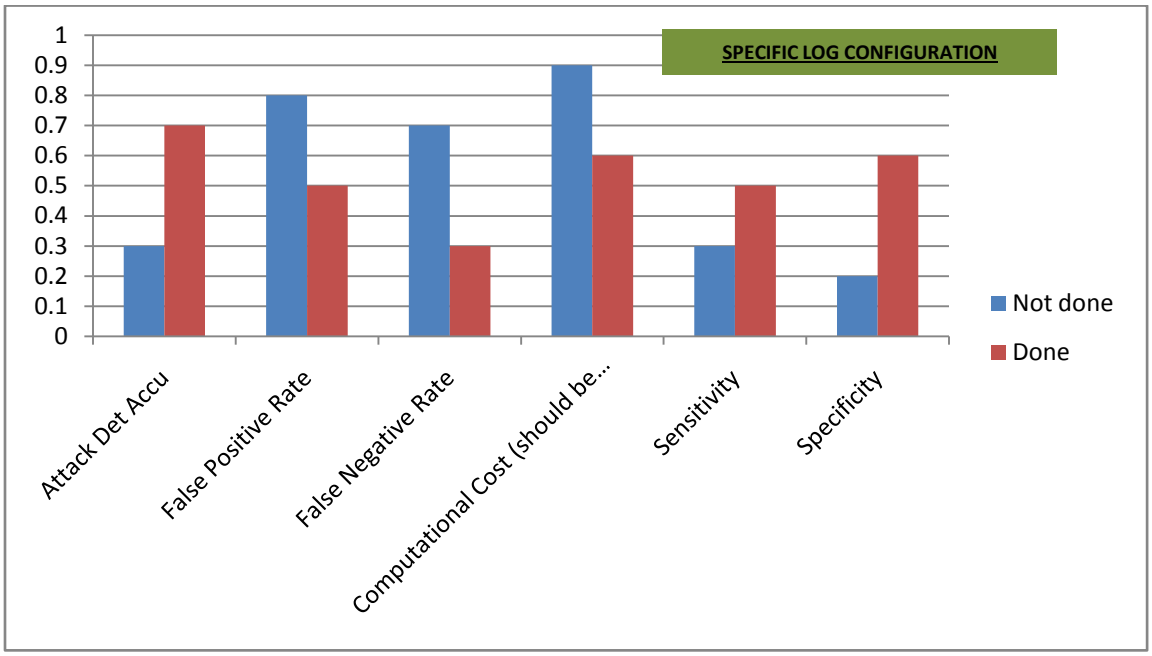

Fig 28. Results of Specific log Configuration

5) Proper Integration with SIEM

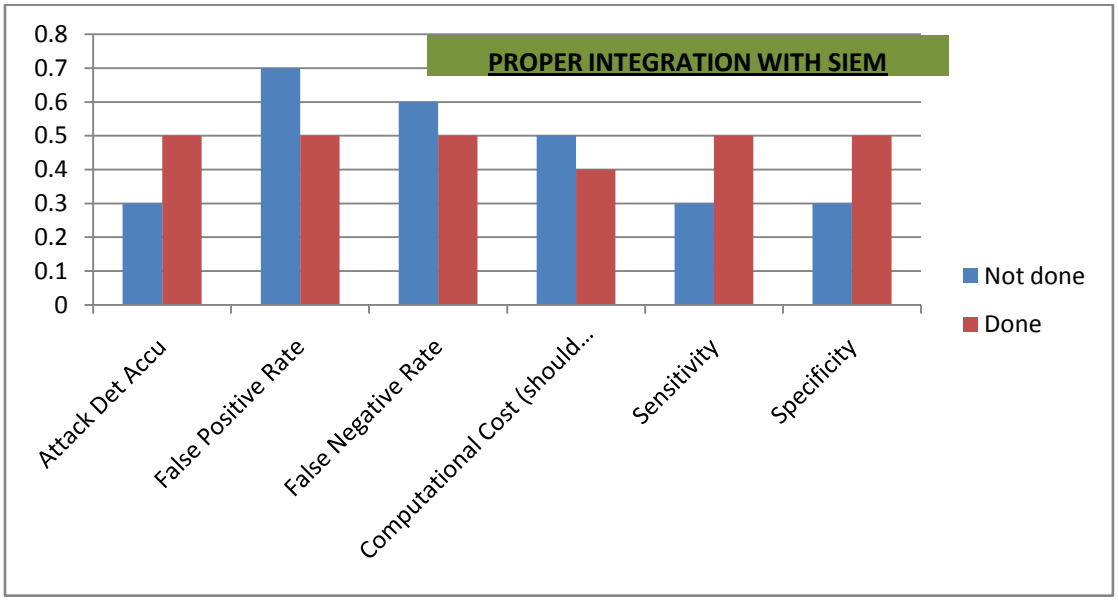

Fig 29. Results of Proper Integration with SIEM

6) Storage Sizing

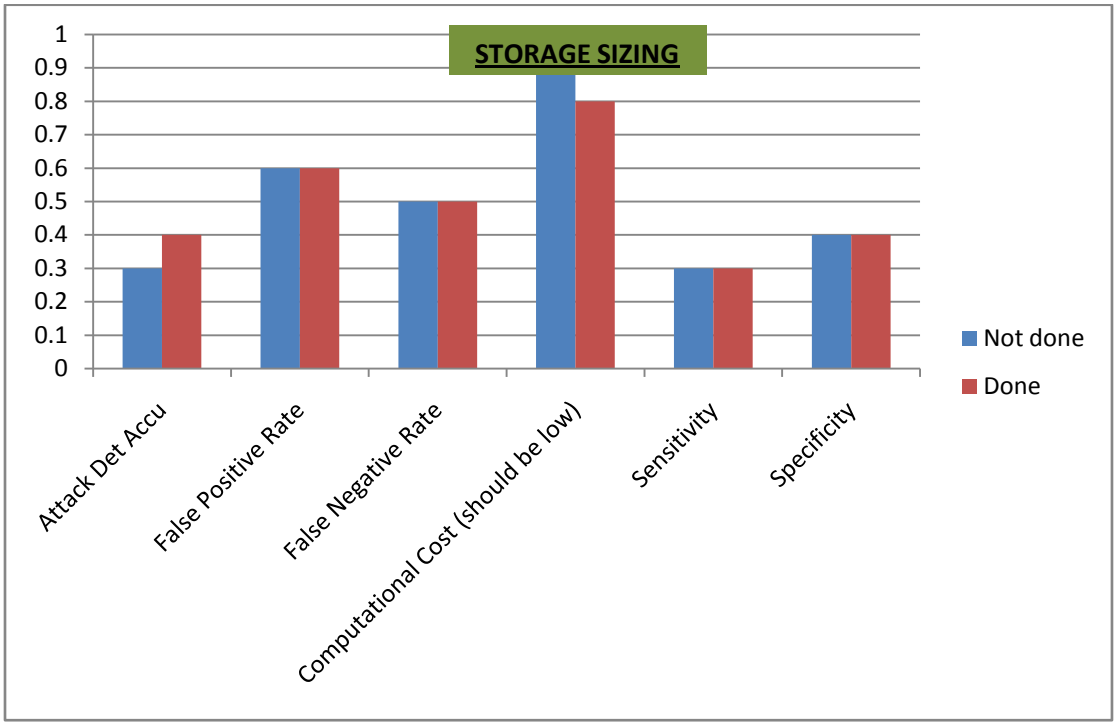

Fig 30. Results of Storage Sizing

7) Source Filtering

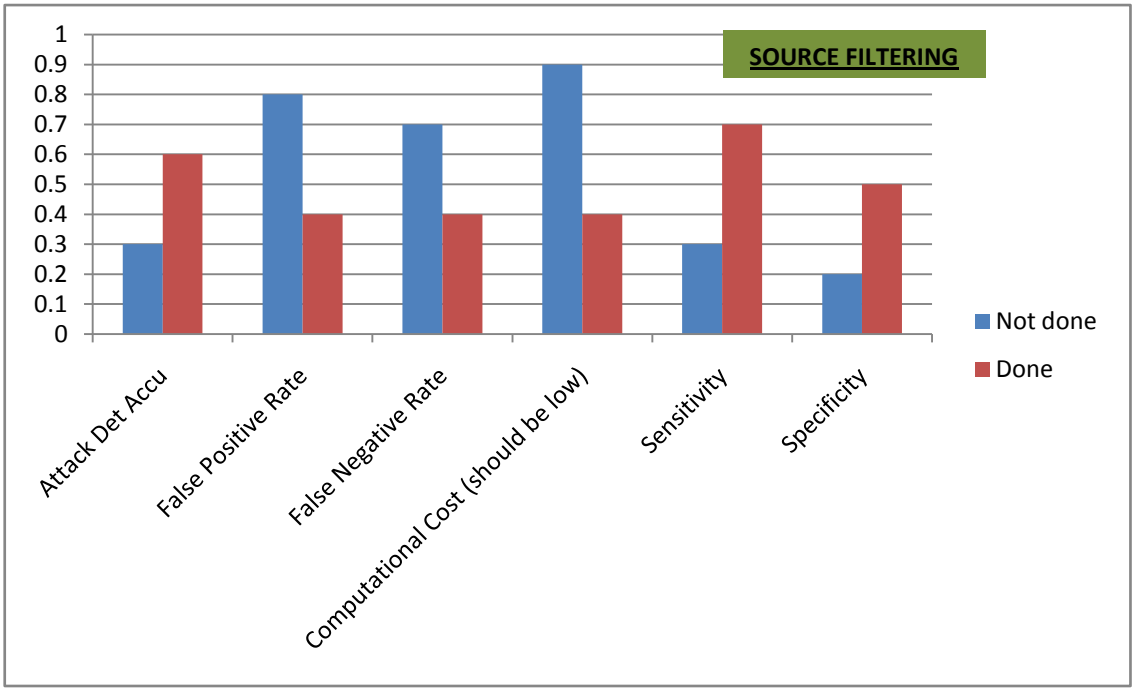

Fig 31. Results of Source Filtering

8) Deployment Methodology

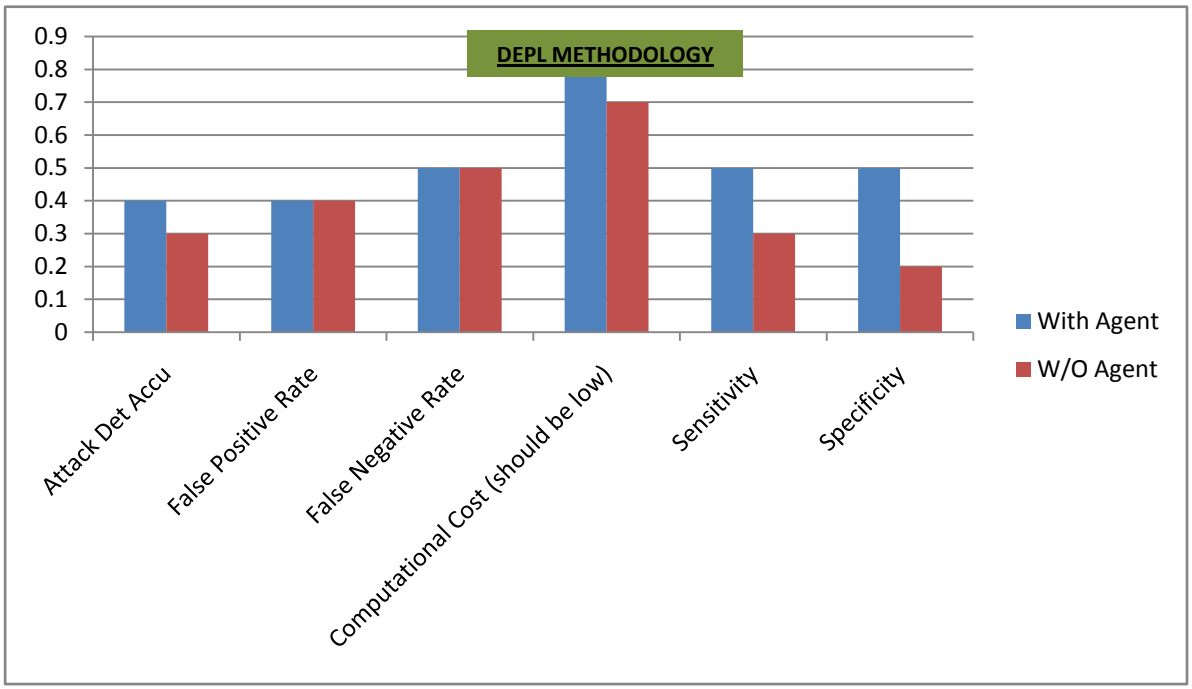

Fig 32. Results of Deployment Methodology

9) Network Hierarchy Configuration

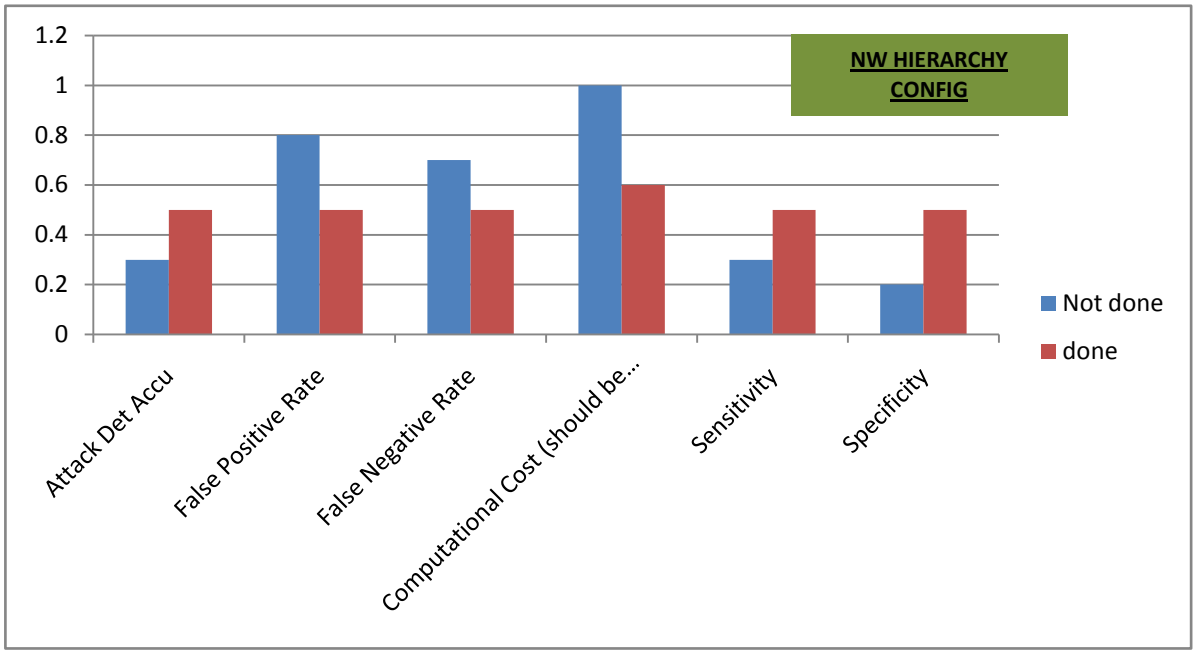

Fig 33. Results of Network Configuration Hierarchy

10) Retention Period

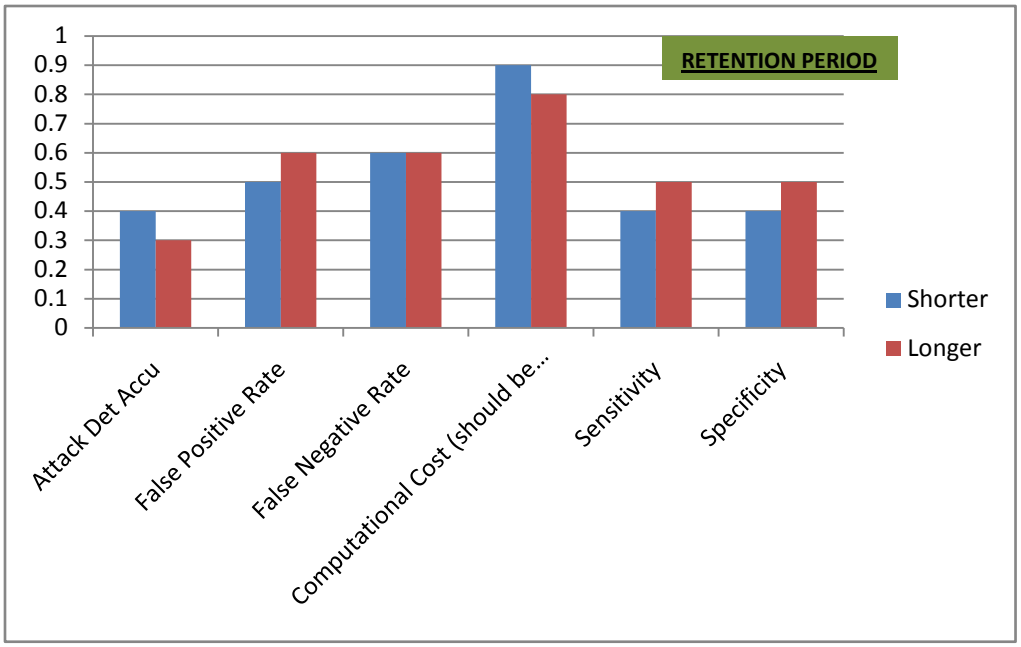

Fig 34. Results of Configuring Retention Period

11) Use Cases

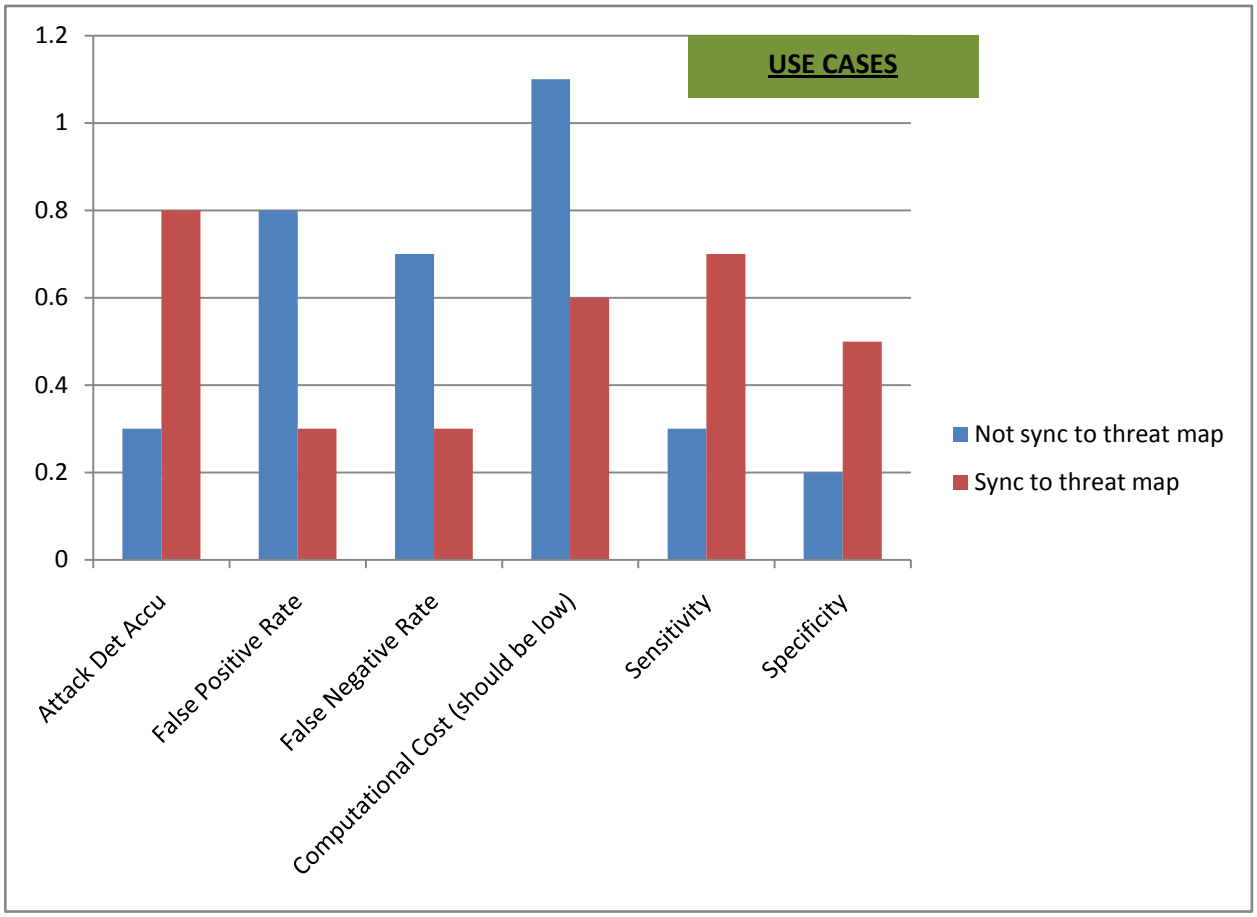

Fig 35. Results of Configuring Proper Use Cases

8.3.4 The Qualitative KPIs

The qualitative KPIs were formulated after carefully scrutinizing the follies and shortcomings mentioned in section 8.1 and were designed as a combination of the requirements surfaced thereafter and the standard metrics in vogue in the IT industry to evaluate SOC performances. A summary of the qualitative KPIs used is as under:

Ser	KPI (Metric)
1.	Provision of feedback within the framework
3.	Repeatable processes
3.	Provide complete linkage to the source of offence: Granularity of detection
4.	Successful creation of reporting chain
5.	Scalablility
6.	Competency development roadmap and training of human resource
7.	Periodic assessment of HR
8.	Documentation of SOC procedures and info flow
9.	Situational risk awareness
10.	Provision of intelligence peculiar to own architecture
11.	Prioritization of Targets
12.	Maintain a baseline configuration specimen
13.	Identification and auth of user activities
14.	Escalation of risk related data, reporting and anomalies
15.	Provide periodic and timely maintenance
16.	Carry out periodic risk assessment
17.	Integration between people, processes and Technology- overall security objective
18.	Provision of minimum use cases
19.	Ensure info sharing b/w Soc and Ops

Table 15: Qualitative KPIs

8.3.5 Results of Quantitative KPIs

The proposed framework was scrutinized for the presence of the above mentioned qualitative KPIs, and the results were proven argumentatively giving references to the relevant sections of the suggested solution. A summary of the results is as follows:

Ser	KPI (Metric)	Framework Analysis against KPI		Reason/Argument		
		Fulfilled	Not fulfilled	Phase	Sub phase	Process/ Feature
1.	Provision of feedback within the framework	Fulfilled		1. Maintenance phase		Improvement and feedback mech
2.	Repeatable processes	Fulfilled		1. Analysis 2. Policy formulation 3. Deployment 4. Maintenance		
3.	Provide complete linkage to the source of offence: Granularity of detection	Fulfilled		1.Analysis phase	a. Selection and re-eval of sec measures	a. selection of security measures b. employment decision c. configuration of security mechanisms
				2. Policy formulation	a. SOC operational policy	(1) . New asset induction and installation policy (2) Coord SOP between SOC and Ops (3) contextual info sharing (4) prior information policy
				3.Deployment	a. Preparatory requirements	(1)Config of specific logs (2)Integration with SIEM
					b.Deployment	(1)Updated asset list

					c. Consolidation	(1) Config of network hierarchy
4.	Successful creation of reporting chain	Fulfilled		1. Policy formulation	a. SOC operation policy	(1) Reporting procedure (2) Defining of authorities
				2. Maintenance phase	a. Reporting and response mechanism	
5.	Scalable	Fulfilled		The process can absorb any number of increase in assets or users. It will remain the same and would not require any changes to its flow.		
6.	Competency development roadmap and training of human resource	Fulfilled		1. Maintenance phase	a. Training	(1) Required qual of manpwer tires for SOC (2) Training and eval methodology
7.	Periodic assessment of HR	Fulfilled		1. Maintenance phase	b. Training and eval	
8.	Documentation of SOC procedures and info flow	Fulfilled		1. Policy formulation phase	a. SOC operation policy	
				2. Maintenance phase	a. Reporting and Response mechanism	
9.	Situational risk awareness	yes		1. Analysis phase	a. Asset inventory and eval	(1) Asset categorization
					b. Threat analysis and risk calculation	
				2. Maintenance phase	a. Reporting and response mechanism	

10.	Provision of intelligence peculiar to own architecture	yes		1. Policy formulation phase	a. Organizational security policy	"this policy dictates the configuration of complete security devices as well as the SIEM tool"
				2. Deployment phase	a. Intelligence	(1) Rules according to security policy (2) Rules covering all attk vectors
11.	Prioritization of Targets	Yes		1. Analysis phase	a. Asset inventory and eval	(1) Asset categorization
					b. Threat analysis and risk calc	(1) Risk calculation
				2. Deployment phase	Intelligence	(1) Formulation of rules according to the threat canvas
12.	Maintain a baseline configuration specimen	Yes		1. Policy formulation phase	a. Security and operational mechanism configuration policy	"defining the baseline configurations which will be maintained in all security and operational mechanisms including SOC/SIEM
13.	Identification and auth of user activities	Yes		1. Policy formulation phase	a. SOC operational policy	(1) Reporting procedures (2) Authorities
				2. Maintenance phase	a. Reporting and response mechanism	
14.	Escalation of risk	Yes		3. Policy formulation	b. SOC	(3) Reporting

	related data, reporting and anomalies			phase	operational policy	procedures (4) Response procedures
				4. Maintenance phase	b. Reporting and response mechanism	
15.	Provide periodic and timely maintenance	Yes		1. Maintenance phase	Improvement and feedback mechanism	
16.	Carry out periodic risk assessment	Yes		1. Analysis phase	a. Threat analysis and risk calculation	(1) Risk calculation
				2. Policy formulation phase	a. SOC operational policy	(1) Monitor procedures (2) Co-ord Sop between SOC and Ops
17.	Integration between people, processes and Technology- overall security objective	Yes		The complete framework covers all the three aspects and is designed to bind them together"- specific parts ensure compliance to overall security objective		
				1. Policy formulation phase	a. Org sec policy b. Security and op mech config policy c. SOC op policy	
				2. Deployment phase	a. Intelligence	(1) Rule creation according to threat canvas
18.	Provision of minimum use cases	Yes		1. Deployment	a. intelligence	(1) specimen use cases
19.	Ensure info sharing b/w Soc and Ops	Yes		1. Policy formulation phase	a. Co-ord SOP b/w SOC and Op	

					b. Prior info policy	
				2. Maintenance phase	c. Improvement and feedback mechanism	

Table 16. Results of Qualitative Evaluation

8.4 Analysis

The above mentioned results of qualitative and quantitative evaluations show that the proposed framework not only efficiently improves the performance of a SOC, but it also mitigates most of the problems faced in the implementation and running of Security Operations Centre, by closed IT organizations. The suggested solution has a unique feature being tailor made for private sensitive enterprises, yet fulfilling most of the industry accepted standards of SOC evaluation. To finalize our analysis of the given framework we made an endeavor to grade it, according to the yardstick of a global standard proposed and practiced by HP [11]. The standard is explained in the following section

8.4.1 Grading

The grading of the suggested framework was conducted according to a standard practiced by HP [11] called SOMM, Security Operations Maturity Model. The model consists of six levels ranging from 0-5. Each level has a title and contains certain characteristics against which the capability of any Security Operations Centre is gauged.

The SOMM model is described as follows:

Ser	Level	Title	Description
1.	Level 0	**Incomplete**	Operational elements do not exist
2.	Level 1	**Performed**	Minimum compliance requirements to provide security monitoring
3.	Level 2	**Managed**	Business/org goals are catered for & processes are repeatable
4.	Level 3	**Defined**	Well defined, subjectively evaluated, flexible in operations
5.	Level 4	**Measures**	Ops are quantitatively evaluated, consistently reviewed, proactively improved.
6.	Level 5	**Optimizing**	Op improvement program implemented to track deficiencies and drive continuous improvement.

Table 17. HP SOMM Model

According to the above mentioned standard, the suggested framework merits to fall in level 5, since it possesses all the characteristics mentioned against each of the preceding levels as well as that of level 5.

8.5 Summary

The evaluation and analysis of the suggested framework proves that the proposed solution can be utilized to efficiently create an organizational SOC which not only caters for the specific short comings and threat scenarios of closed IT organizations but also satisfies the industry standards practiced in relation to SOC.

Chapter 9

CONCLUSION

Closed IT organizations, face a very different attack scenario and have a unique threat canvas as compared to their commercial counterparts. Therefore, the existing SOC frameworks that have been developed on commercial requirements cannot be blindly implemented on these organizations. In all the instances where this has been done, the SOC has failed to achieve its desired objectives. This thesis presents an extensive framework for establishing and maintaining SOC, which has been peculiarly designed keeping in mind the architectures and threat scenarios of closed IT organizations specifically. Moreover through detailed evaluation of the suggested framework against industry accepted key performance indicators (KPIs), the workability and effectiveness the proposed solution has been proven. It is hoped that those closed IT organizations which establish and maintain their SOCs basing on our proposed framework, would not only be able to achieve their desired results, but would also be able to gain a proactive monitoring, threat awareness and reactive capability against attacks on their IT infrastructures.

9.1 Future Work

The concept of establishing, running and maintaining an efficient Security Operations Centre is extremely wide and no one thesis or research product can sum it up concisely. Consequently there is always room available for further improvement and research into newer concepts that could improve the performance of SOC. A few such topics are suggested as under for future researchers to make an effort upon

The topics which, in our opinion need further research are as under

9.1.1 Establishment of a CIRT, specifically designed to be a part of SOC.

Computer Incident Response Teams are an independent and separate phenomenon, when operated in isolation. However in the backdrop of Security Operations Centre they have a peculiar structure and job to perform. Presently no single framework or standard is available which streamlines how a CIRT will operate within the overall structure of SOC.

9.1.2 **Forensics Within Security Operations Centre**.

Forensics is a completely separate field when carried out independently. But within the framework of SOC, forensics has a very different methodology of operation as well as a different mandate, and it usually pertains to log forensics. There is tremendous room of research on how to conduct forensics and establish forensic teams for operating within a SOC.

9.1.3 **Auditing procedures in Security Operations Centre**.

The present literature lacks any standard document which streamlines, as to how to conduct audit of IT organizations through SOC, and how should audit teams be formulated and operate within the overall framework of SOC.

9.1.4 **Detailed Training Framework for SOC Resources**.

Any SOC thrives and succeeds on the manpower and resources which operate it. Therefore the training regime and capability development of SOC resources is of paramount importance. A detailed research can be conducted as to what all aspects are required for the SOC resources to be trained in. Moreover a granular and universal capability development model can be suggested, which can be equally implemented across all kinds of SOCs.

9.1.5 **Reducing false positives in SOC through Big Data Analysis Techniques**.

The biggest impediment in the efficient performance of any SOC is the huge quantum of false positives that is encountered. This quantum not only seriously recedes the response capability of this organization but also causes an overburden to the resources manning the SOC. The characteristics of huge quantity of logs make them resemble the concept of Big Data. Throughout the world extensive research is being carried out on Big Data Analysis. It could prove very beneficial if the existing Big Data Analysis techniques are utilized inorder to reduce the false positives within a SOC.

BIBLOIGRAPHY

[1] Sandeep Bhatt, Pratyusa K. Manadhata, and Loai Zomlot | Hewlett-Packard Laboratories, "The Operational Role of Security Information and Event Management Systems", *IEEE Security and Privacy*, pp.35-41, Sep/Oct 2014.

[2] Stef Schinagl, Keith Schoon, prof. Ronald Paans Ph.D, "A Framework for Designing a Security Operations Centre (SOC)", presented at the 48th International Conference on System Sciences, Huwaii, U.S.A, 2015.

[3] www.hackmageddon.com

[4] ISACA Conference Survey," State of Cyber security: Implications for 2015", Internet: https://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf, 2015[aug 2016].

[5] McAfee Foundstone Professional Services White paper, "Creating and Maintaining a SOC", Internet: www.mcafee.com/ca/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf, Sep 2013 [Sep 2016].

[6] Alissa Torres, "Building a World Class Security Operations Centre - A Road Map", SANS Institute White Paper, Internet:www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907 , May 2015[Jun 2016].

[7] E. Eugene Schultz, Ph.D., "Continuous Monitoring: What It Is,Why It Is Needed, and How to Use It", SANS Institute White Paper, Internet:www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-is-needed-35030, June 2011[Jun 2016].

[8] Kelley Dempsey, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scholl, Kevin Stine, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations", NIST Special Publication 800-137, Sep 2011.

[9] Asieh Mokarian, Ahmad Faraahi, Arash Ghorbannia Delavar, " False Positives Reduction Techniques in Intrusion Detection Systems-A Review", *IJCSNS International Journal of Computer Science and Network Security*, VOL.13 No.10, pp.128-134, Oct 2013.

[10] M. E. Elhamahmy, Hesham N. Elmahdy and Imane A. Saroit, "A New Approach for Evaluating Intrusion Detection System", *CiiT International Journal of Artificial Intelligent Systems and Machine Learning*, Vol 2, No 11, pp.290-298, Nov 2010.

[11] Hewlett Packard Laboratories, “Measure Your Security Operations Centre Capability”, Solution Brief, March 2016.

[12] Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, Will Robinson, “Performance Measurement Guide for Information Security”, NIST Special Publication 800-55 Revision 1, July 2008.

[13] Joint Task Force Transformation Initiative, “Security and Privacy Controls for Federal Information Systems and Organizations”, NIST Special Publication 800-53 Revision 4, Apr 2013.

[14] Gary Stoneburner, Alice Goguen, and Alexis Feringa, “Risk Management Guide for Information Technology Systems”, NIST Special Publication 800-30, Jul 2002.

[15] J. Michael Butler, “Benchmarking Security Information Event Management (SIEM)”, SANS Institute White Paper, Internet: www.sans.org/reading-room/whitepapers/analyst/benchmarking-security-information-event-management-siem-34755, Feb 2009[Aug 2016].

[16] Erkan Kahraman, “Evaluating IT Security Performance with Quantifiable Metrics”,Internet:www.citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.4000&rep=rep1&type=pdf, [Aug 2016].