Int. J. Nonlinear Anal. Appl. 12 (2021) No. 2, 869-895
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2021.5145

Grasp on next generation security operation centre (NGSOC): Comparative study

Yau Ti Dun[a,c], Mohd Faizal Ab Razak[a,*], Mohamad Fadli Zolkipli[b], Tan Fui Bee[a,c], Ahmad Firdaus[a]

[a] *Faculty of Computing, College of Computing and Applied Sciences, Universiti Malaysia Pahang, 26600 Pekan, Pahang, Malaysia*
[b] *School of Computing, UUM College Arts & Sciences, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah Darul Aman, Malaysia*
[c] *Sysarmy Snd Bhd, Wisma Zelan, No 12, 1, Jalan Tasik Permaisuri 2, Bandar Tun Razak, 56000 Kuala Lumpur, Federal Territory of Kuala Lumpur, Malaysia*

(Communicated by Madjid Eshaghi Gordji)

Abstract

With the growing number of cyber security threats affecting the business environment of many organizations, especially the IT environment. With the growing number of cyber security threats affecting the business environment of many organizations, especially the IT environment. Managed protection systems, including SOC, are highly sought after. Managed protection systems, including SOC, are highly sought after. The problem with SOC is that when building up their own SOC or hiring a third-party to provide SOC, organizations are not able to apply adequate criteria or standard frameworks. The aim of the study is to lay the foundations for developing a modern system of systematic operation centers for the next generation (NGSOC) for IIoT climate. This paper contains thorough, qualitative literature survey on the implementation of a Security Operation Centre (SOC). A comparative study is carried out using a variety of previous research sources and a literature review. The findings from the report show that previous research is not adequately guided, especially in the safety and technical aspects of the building block of the SOC. It is hoped that by proposing the framework, cybersecurity threat prevention and identification would be strengthened even further. The success of the NGSOC will ultimately be determined by the integration of individuals, procedure, and technology.

Keywords: SOC, SIEM, IIOT, Security, NGSOC
2010 MSC: Primary 90C33; Secondary 26B25.

[*] Corresponding author

Email addresses: alan@sysarmy.net (Yau Ti Dun), faizalrazak@ump.edu.my (Mohd Faizal Ab Razak), m.fadli.zolkipli@uum.edu.my (Mohamad Fadli Zolkipli), fuibee@gmail.com (Tan Fui Bee), firdausza@ump.edu.my (Ahmad Firdaus)

Received: February 2021 *Accepted:* April 2021

1. Introduction

The 2017 Internet Security Threat Report of Symantec Corporation shows that over 7.1 billion identities are exposed to data infringements [1]. The 2017 Internet Security Threat Report of Symantec Corporation shows that over 7.1 billion identities are exposed to data infringements [1]. Cyber-attacks have wreaked havoc on an unparalleled scale. To make a big effect, attackers often used very basic tools and tactics. A Security Operations Center (SOC) is generally a department set up to maintain the security of an organization. In practice, a SOC is a community of people who monitor, analyze and safeguard the information system of an entity such as servers, networks, databases and more [2]. Simultaneously, the Industrial Internet of Things (IIoT) nation, where it is in a company's best interest to hire highly skilled workers. professionals who are well-versed in the technology they endorse and use on a regular basis. They must understand and be proficient in the use of Security Information and Event Management (SIEM) systems, loggers, physical security infrastructure, Protocol analyzers, Intrusion Detection Systems (IDS), and vulnerability scanners, to name a few, must all be capable of dealing with today's cyber-threat setting. They will need to be aware of the method of collecting data from these sources and of how to correctly increase stakeholder security concerns.

So what are really the things we don't have? Eight people died and 48 others were injured on the 3 June 2017 London Bridge terror attack. The government's intelligence body has some major shortcomings, according to the security analysts' study. They stressed the large amount of intelligence data available in a number of sizes and sources. These could all be combined to form a comprehensive intelligence picture, including terabytes of data, talks and CCTV vidéos. The information was provided but the information in the intelligence activity, which enabled attackers to radar, could not be proceeded, interpreted or contextualized [3]. Cyber-assaults, such as advanced persistent attack (API) are increasingly being targeted, complex and technically advanced (APT). Managing too many incidents can be disastrous and time-consuming for most organizations [4].

In general, there are current IT companies frameworks and best practices such as CoBIT 5, ITIL and ISO/IEC 27001:2013. Neither, however, is tailor-made for the SOC system. Several studies [5] identified SOC problems and limitations that can be further categorized into the following categories [2]:

a) **People**

   - There is a scarcity of security professionals who are both trained and experienced.
   - Ineffective management and a lack of financial responsibility

b) **Process**

   - Most software come with a collection of default correlation rules that aren't always the best fit for a particular situation.
   - In the current phase, there is a lack of constructive reaction.

c) **Technology**

   - Instead of a scientific method, the choice of technologies and techniques depends on the market.
   - The basic line to pick SOC tools is not sufficient

Frost & Sullivan is a consulting firm. By 2020, the industry expects a shortage of 1 5 million ISO professionals and cites the major problem as looking for adequate staff [6]. While the NGSOC retains the capability to detect threats, it is a model that is aimed at identifying new threats that have not been identified on any previous basis. To achieve this capability, organizations must invest in the correct areas and integrate their available resources.

NGSOC uses an approach that involves security enforcement points and analysis approaches on threats, rather than concentrating on security endpoints. Instead of focusing on security endpoints, the NGSOC employs a security enforcement and analytical approach on risk [2]. Building a high-level NGSOC takes considerable time and resources. The work is therefore considered more of a sprint than a marathon. The initial motivation for this study is to seek a shared methodology in helping organizations develop their own internal NGSOC or providing guidelines for the involvement of NGSOC third-party providers. The main reason for the NGSOC requirement is that cyber security risks are reduced to the lowest possible.

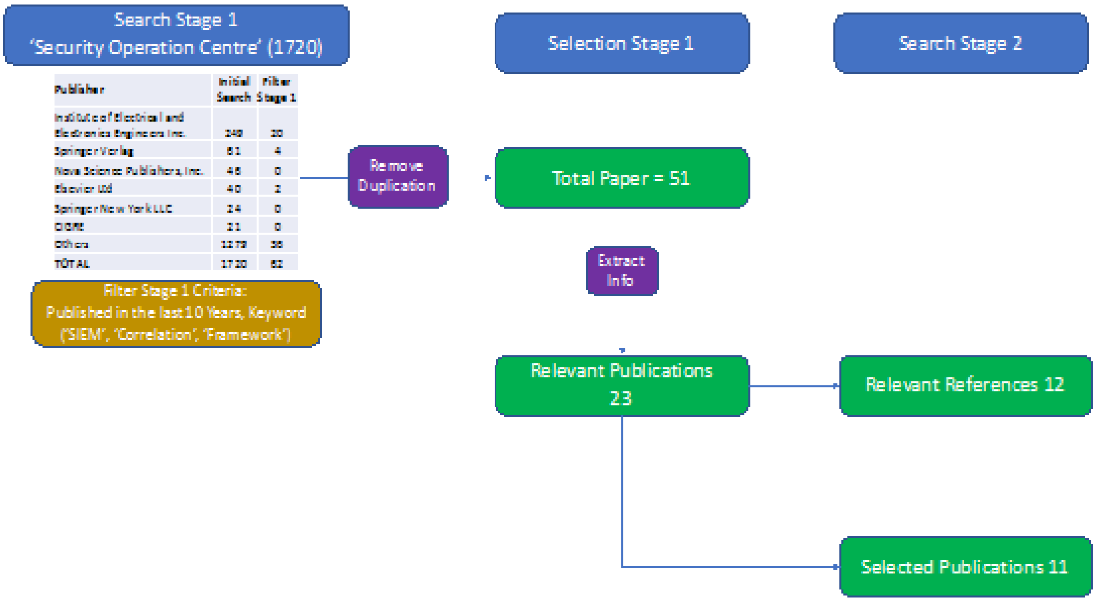
In this study, a large qualitative literature survey will be conducted to investigate existing SOC and cybersecurity practises. A new NGSOC system will be proposed to provide organisations with comprehensive guidance for acquiring or implementing NGSOC. To summarise, a specialised NGSOC with the appropriate technology, processes, and qualified personnel must be established as a central component at the heart of a successful incident response process. SOCs need coordinated cross-disciplinary teams with very specialized skills in the fight against advanced cyber threats. Such skills and qualified staff in the safety community are therefore severely lacking in developing, operating, and sustaining SOCs.

The following is the structure of this paper: The methods of systematic observation and a literature review on the subject are covered in Section II. Section III includes a compilation of previous work and the SOC model, which is divided into six categories: stakeholder, governance, stability, technological, functionality, and intelligence. The intentional contribution to comparative analysis is discussed in Section IV and conclusions are discussed in Section V.

2. Methodology

The primary concern is evaluating previous research approaches to carrying out SOC practises. Since this is a non-empirical analysis focused primarily on extensive library studies, a comparative method of evaluation is used as the primary tool. A data extraction process was carried out in order to pick a range of publications for the comparative analysis. The stages of data extraction are depicted in Figure 1 below.

There are three stages which are: Search Stage 1, Selection Stage 1 and Search Stage 3, the first step is by searching on Scopus, the abstract and citation database, with the keyword 'Security Operations Centre' The first step. From this initial search a total of 1720 papers emerged. Further indexing is carried out on the parameters reported in last 10 years and filtered with three other keywords, including 'SIEM,' 'Correlation' and 'Framework,' in the Computer Science Topic Journal. The results of the quest for 'Searching Stage 1' are sorted by the name of your publisher. We may identify from the sorting method the top 6 publishers that actively publish research on SOC. The



Publisher	Initial Search	Filter Stage 1
Institute of Electrical and Electronics Engineers Inc.	249	20
Springer Verlag	61	4
Nova Science Publishers, Inc.	46	0
Elsevier Ltd	40	2
Springer New York LLC	24	0
CIGRE	21	0
Others	1279	36
TOTAL	1720	62

Figure 1: Data Extraction Stages

total number of papers in the first stage is 51 after removing duplicates.

'Selection Stage 1' entails a systematic study and analysis of 51 pieces of literature. Then, 23 papers out of 51 are chosen as important publications. Finally, 11 papers are summarized and selected for the comparative analysis, and 12 other papers are selected for the purpose of comparative study. Due to its similarities to the SOC model, the remaining paper from the three stages was chosen. In this section, we will examine in detail the descriptive comparison, analyze the characteristics, strengths and weaknesses of each SOC model. Following that, this paper presents the study in the form of a figure for easier understanding and visualization. It is anticipated that future research will develop a structured structure through comparative analysis.

3. Related work

A general literature review reveals that the SOC consists of three key elements: personnel, process, and technology. Because the cybersecurity climate is evolving constantly, it is crucial to understand the current policies, processes, and controls in the industry and how these elements are monitored. The comparative research aims at developing a model theoretical framework that can withstand validation by testing in different practical environments and current results.

4. Stakeholder

A stakeholder is an individual or group of people who have an interest in and may influence or be influenced by a corporation. NGSOC stakeholders include the service acquisition firm, customers, business partners and NGSOC personnel, contractors, and consultants. NGSOCs need to be established and maintained to protect their businesses.

4.1. Stakeholder Requirements

Every day, each company manages a large amount of data in its daily operations. This led to the need for automation and convergence in cyber-attack prevention, detection and response [8]. Real-time monitoring of security incidents achieves the following objectives:

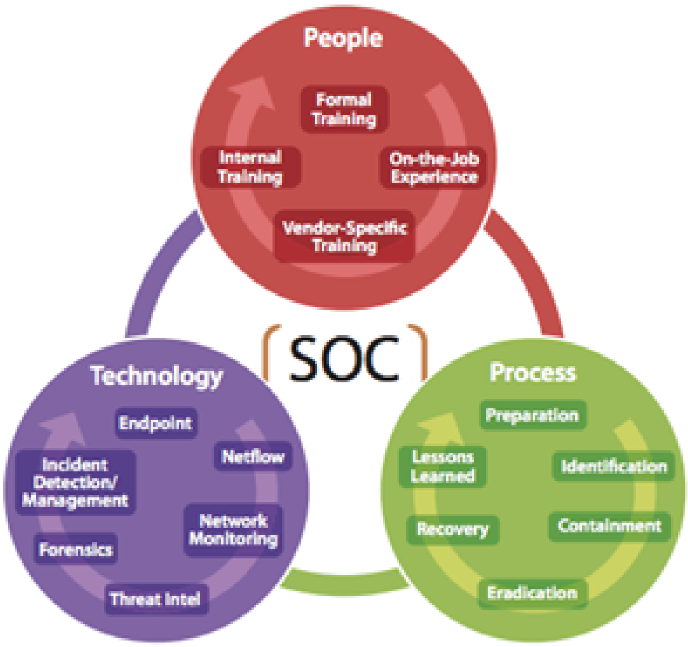


Figure 2: Building Blocks of NGSOC. Reprinted from "Building a World-Class Security Operations Centre: A Road Map", [7]

- Security accidents identification (incidents); device vulnerabilities detection; quality management of safety measures ensured.
- • Provide forensic evidence for cybercrime investigations.
- • Control over the method of change management.

According to Schinagl, Schoon, and Paans [9], the commercial interests that must be covered are the organisations' clients and partners. Moreover, a classification of data exchanged between these parties includes privately, confidentially or financially related information, which is an exchange of information to be protected. According to the policy criteria of the Bank Negara Malaysia [10], financial institutions need to improve SOC capacity. This requires constant monitoring in order to detect anomalous behavior, recognise potential breaches and enforce successful reactions. In addition, penetration tests, vulnerability assessments, malware detection and forensics must be carried out.

A number of authoritative documents and normative documents provide for monitoring when required It is essential to consider the legal and regulatory provisions which may influence the type of information which can be collected and monitored before interacting with any activities involving the owners of the information. In certain situations, the customer must obtain the consent before his data can be processed. In general, the law will require financial institutions to track certain information. These requirements differ from country to country. The goal of this research will therefore be to find a common ground that most organizations would use to deal with SOC [11].

4.2. Service Management

SOC establishes a written agreement with their customer about their particular level of service as a service provider. By establishing a set of quantifiable goals, they work together to define and agree on an appropriate standard of service [12]. The following are the components that can be measured:

- Incidents are events that occur when a certain condition is exceeded.
- Outages: An occurrence that causes an activity to become inaccessible.
- Downtime refers to the amount of time that has passed since an event occurred.
- Availability refers to the amount of time a service is available for use.

These priorities are part of a service level agreement (SLA). This contract also provides detailed definitions of the duties, responsibilities and contracting services provided by the SOC. If the service is provided at the expected standard, it should also specify explicitly the remedies or penalties that are in effect. Additional observable data:

- • The SIEM log list should indicate that logs should be included.
- The average time it takes to operate a new log source.
- The accumulated number of minutes that such devices could not submit logfiles.
- The cumulative number of minutes without operation for all applications is
- The accumulated time the SIEM did not receive log files.
- The number of cases of threat identification increases (minimum 20 cases for priority assets, 10 cases for the lower priority system). The number of assets without a minimum number of cases of use is also increasing.
- The total number of threat models for an asset that do not have the required number of cases of SIEM use.

Miloslavskaya [13] suggests that SOC integrate safety events with SLA criteria, since it is important for companies because it helps to evaluate damages arising from an affected network or other offsite events. SOC also creates business models and analyses the effect of various security incidents on these models, according to the article. The determination of asset costs, on the other hand, would be a clear disadvantage of this approach.

a) SOC services have their own Service Level Agreement (SLA) and Key Performance Indicators (KPI) like all other services, which determine the ROI (ROI). The following indicators can be relevant for senior management, according to [14].

b) The cumulative number of events uncovered over time.

c) False positives, false negatives, true negatives, and true positive are all numbers that can be used to measure the number of false positives, false negatives, and true negatives.

d) Top 5 or 10 cyber-attacks by country of origin, nation-state funding, capability and severity

e) Internal policy breaches, noncompliance, and the severity of exposures are summarized in this report.

f) Misuse and harassment of privileged users in a nutshell

Security administration, incident response, security monitoring, regulatory assistance, remediation, security infrastructure, security roadmap and planning, digital forensics, threat research, eDiscovery and collecting legal proof are just some of the SOC's services [8]. Around the same time, companies and their service needs evolve over time. Rather than being regarded as a static text, SLA should be revised on a regular basis. The following are some of the variables that may influence the changes: customer's business expectations measurements, calculation methods, and procedures workloads technological climate.

In terms of SOC capabilities, the monitoring service is a significant activity. Some SOCs have security analysts monitoring the service around the clock, 24 hours a day, seven days a week, while others control during business hours, usually from 9:00 a.m. to 5:00 p.m., with on-call Level 2 and Level 3 support for major incidents, while still others run only during business hours, with no support. It's important to remember, however, that the SOC's operational structure is determined by business needs and the security policy of the company [14].

NGSOC Management

Grobler, Jacobs, and Niekerk [11] talk about two different ways to provide SOC services:

- **Internal SOC**
  SOCs that serve an organization's internal security requirements are described as SOCs. Only one consumer is served by this model. There are two types of deployments: clustered and distributed (global service requirements)

- **MSSP (Managed Security Service Provider)**
  Security devices and systems, such as the IPS and firewall, are monitored and managed remotely. This model caters to a variety of customers from various sectors, as well as from different countries in some cases.

SOCs are sometimes treated as one SOC, regionally or through the cloud, according to a survey study [8]. Most respondents' SOCs (61%) are currently clustered in one location. As shown in Figure 3, the second largest group (28 percent) said their SOC functions were spread through various security and response units, while 25 percent said their SOCs were centralized and distributed regionally, and 17 percent said they brought all their SOC functions into the cloud. The blue bar indicates an organization with its headquarters in the United States, while the red bar indicates an organization with its headquarters in Europe.) SOCs may be incorporated into a company's internal operations or outsourced to a third-party supplier. The benefits and drawbacks of these alternatives [13]:

The SOC model, according to a previous study [4] has seven dimensions. The categorization is based on an initial visit to the operation center and the collection of data. The following measurements are included:

i. **Scope**
   SOC is defined in terms of its sphere of influence, economic or government sector, functional position, functional operation, speed, and size by the scope dimension. The model is made up of the following main elements: effect emphasis, field, power, size, functions, functional abstraction, response form, and response timeline.

ii. **Activities**

   a) <u>Protection</u>
      Routine procedures, system administration, installation and configuration management,

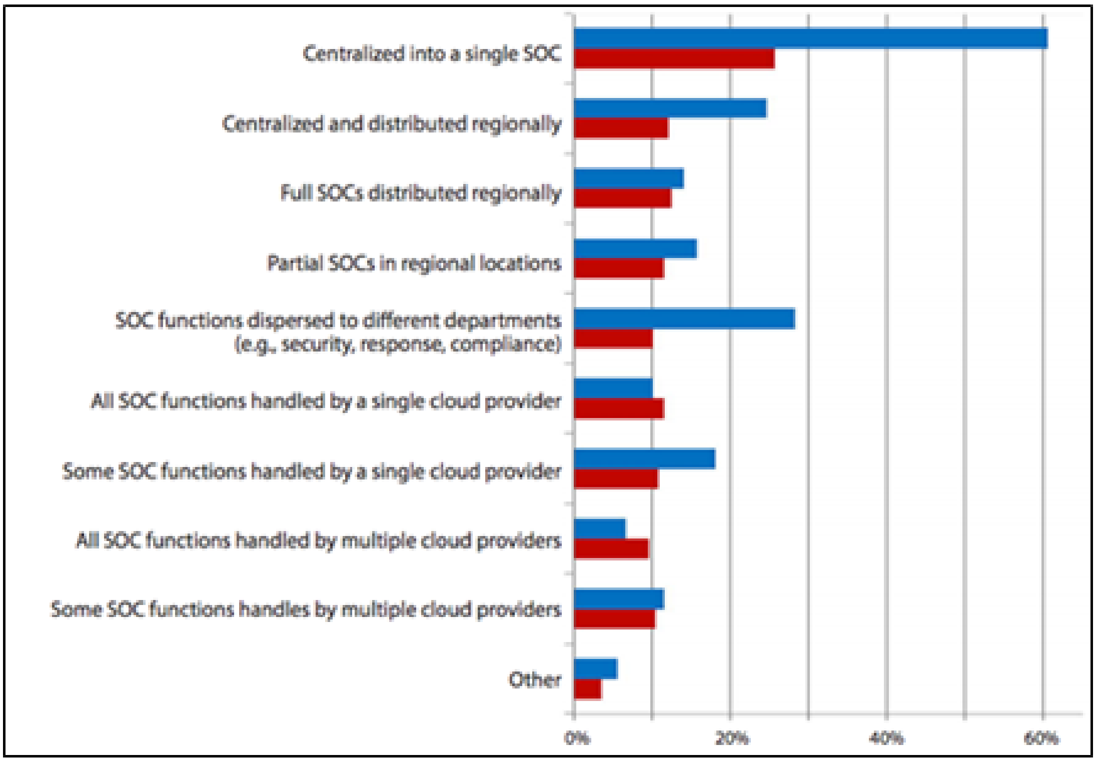


Figure 3: Location and Centralization of SOCs, 2017 .

formal training, monitoring and planning of infrastructure are all part of infrastructure management.

b) Incident Management
Procedures, acts, and practices for detecting, reporting, analyzing, informing, cooperating, and responding to incidents.

c) Analysis
Information about missions, user activities, use, traffic, performance accidents, risks, vulnerabilities, security systems, and incident management are assessed using a collection of protocols, acts, and activities.

iii. **Organizational Dynamics**
The following factors influence how a company changes over time: growth rate, sustainability, organizational change, project transformation, and source of funding.

iv. **Facilities**
Installations are distinguished by room size, number of desks, overload capacity, operating hours, configuration style, variety of continuity, ongoing organizational preparation (COOP) and methods of teamwork.

v. **Process Management**
The level of application and ongoing changes in standard practices in organizations was founded on four factors: training and qualification, successful use of SOPs, development, and analysis.

vi. **External Interactions**
SOC-sponsored formal, informal relations. The willingness of the center to listen and react to

Table 1: Pros and Cons of Server Location

	In-house	Outsourced
Advantages	Better understanding of their own environment, more effective, easier customization, improved correlation process, and more affordable pricing of tools.	Often less expensive because there are no upfront costs, more impartial because there are more experienced resources available, less chance of corruption, and unbiased.
Drawbacks	Significant investments are required, there is a high risk of collusion, and large-scale trends are less likely to be recognized as compared to specialized third-party experience.	There is less information about IoTI; staff is less vigilant; there is a chance of external data mishandling; and there is no long-term benefit for IoTI.

events influences these interactions. Six outside organizations are: emergency, international, trade, government, law enforcement, and intelligence.

vii. **Environment**
In the SOC's operating culture, the atmosphere has an impact. There are six characterization factors for the environment: visibility, scope, data handling, capacity, stability external and communication within the group.

Stakeholder Reporting

He has indicated that reports should be customised for user groups in a study carried out by [14]. It is enough to provide a summary of the security position on a 'high standard' basis for senior management. However, the reports need to be altered from a technical point of view for system administrators, security architects and SOC managers in order to avoid further and potential events. The criteria for stakeholder reporting were not stated however, the criteria for inclusion in technical reports are:

a) Attack date and time

b) Reference date, time and log

c) Malware name, application stream identified and compromised path

d) Geographical IP position of the source of the fraudulent transaction risk ranking, data stream

e) Entity ID, traffic ID, IP address, system ID of boundary, exploit-invoked order

Governance

Governance aims to improve information technology management and control (IT) in the interests of primary stakeholders. The Board of the company has a responsibility to ensure the good governance of IT along with other key business functions. COBIT 5 is a structure for IT governance [15], outlining five concepts such as:

i. **Meeting Stakeholder Needs**
There is a company to build trust and provide its stakeholders with value.

ii. **Covering the Enterprise End-to-end**
Covers all company tasks and procedures. Instead, they consider information and related technology as an asset which must be handled by anyone inside the company just like every other asset.

iii. **Applying a Single Integrated Framework**
A company may choose to comply with other recent and applicable norms, for example ITIL series, TOGAF and ISO/IEC 27000.

iv. **Enabling a Holistic Approach**
Systemic control by interconnected facilitators.

v. **Separating Governance from Management**
In terms of function and organizational structure, the two were clearly distinguished.

It is the board's duty to ensure that cyber threats are mitigated. Lenders, regulators, and consumers are all accountable. Adopting governance values that invest in people and emphasize collaboration leads to sustainable governance. Therefore, operating an operation center is not a one-person affair and as such, industry company must cooperate and exchange information that will allow better detection and prevention of attacks.

Facilities Management

When designing SOC facilities, the following considerations must be considered [4]:

- Physical space scale; number of seats available for SOC employees; potential for staff expansion during high-priority events; operating hours
- Resource's layout and physical settings (personnel, equipment, and furniture).
- Percentage of continuity resources.
- Dedicated resources time can be put into action if necessary.
- Methods of communication.

People Management

The modern SOC business is hierarchically organised around SIEM scheme, according to Bhatt, Manadhata, and Zomlot [16]. In general, SOC consists of a number of security analysts (SA). At present, three stage SA are best practised. The team works 8-12 hours a day around the clock. Due to their long working hours and the enormous workload for Level 1 SAs, the duration of retention is also short, including training for less than two years. The security analysts' roles and responsibilities are shown in the table below.

At present there is little talent pool available for trained analysts. As the SOC employees' skills and expertise are far more critical than investing in tools, the organizations need to resolve this deficiency. Since cyber-attack is increasingly sophisticated and complex, SOC must rely heavily on a human element in order to protect cyber space. SOCs need the Chief Information Security Officer (CISO), who reports to the Chief Information Officer, to have a solid organization (CIO). They work together in accordance with the organization's mission and security objectives [9]. The employees of SOC have to deal with the constantly changing world, so training is necessary to fulfil their tasks [7], as stated in Table 2.

When new workers are hired for the SOC, they will receive on-boarding training that includes functional training, security awareness, and a security culture program [17]:

Table 2: Security Analysts Roles

Security Analysts	Duties & Responsibilities
Level 1	• Monitor the SIEM system alert screen • Triage events (decide event's severity level) • Escalate rules to SOC engineer/higher level SA in case of high number of false positives • Escalate alert for further investigation for when they can't classify an alert as either an attack or false positives
Level 2	• Maintain vigilance over the SIEM device alert screen. • Events are prioritized (the intensity level of the incident is determined). • If a large number of false positives occur, escalate the rules to the SOC engineer/higher level SA. • If they are unable to classify a warning as a false positive or an attack, they escalate the alert for further investigation. • Examine the alerts that L1 SAs have mentioned as potential attacks. Prepare a case study • Make a case and send it to the forensic team (if breach is identified)
Level 3	• Assemble a forensic team and security engineers • Determine the scope and effect of the attack. • L2 can be used to fine-tune rules to minimize false alarms.

i. **Functional training**
A fundamental training to learn the process, resources, strategies, laws, and regulations of the organization.

ii. **Security awareness**
The main goal of education is to minimize the likelihood of social engineering assaults. The information security chain is usually referred to by employees as the weakest link. So routine situational drills, safety knowledge and social engineering assessments are critical.

iii. **Security culture**
A long-term campaign is the development of a security culture. It involves more than a person's safety. The whole team can work together and efficiently interact. In case of a suspicious incident, employees should be encouraged to inquire, inform, report and act accordingly. To allow them to comply with the rules and protocols, they must be informed about the sanctions and implications of data leakage or security infringement.

Operational Management

The operating configurations of each SOC will be different. In other words, one approach does not inherently apply to another to the detection of cyber threats. It is important that your aims, your risk appetite and the environment are understood according to each individual organization. A SOC may involve individuals with a range of skills, processes and even use technology. A SOC may depend on a third-country service provider or have hybrid capability [9]. This research will take account of parameters relating to human processes and technology to create NGSOC to decide the optimal solution for each organization. SOCs can generally be divided into two different types of operational methodology as defined in Tables 4 and 5 regarding counteraction capacity and deployment scenarios:

[9] found there is no broadly adopted structure, as most SOCs are organic, designed and implemented in a specific manner. Processes implemented by security experts that they believe is the solution to their company's objectives. Processes build best-in-class processes with the support of available resources (e.g. safety knowledge, financing, prior experience). Much IT departments are SOCs. Various SOC formats [9] for example: The following are:

i. **Integral SOC:**
Analysts and consultants involved in developing safe services would later perform compliance scanning and continuous monitoring. Additionally, SOC offers infrastructure assistance. This structure enables the most effective exchange of information.

ii. **Technology driven SOC**
Infrastructure support and activities should be prioritized. Near coordination with engineers in the operational environment leads to greater effectiveness.

iii. **Partly outsourced SOC**
In terms of size and capacity, infrastructure and workers are limited. As a result, monitoring and scanning services are contracted out to a third-party vendor. Information exchange and teamwork are relatively weak because of the outsourcing relationship.

iv. **Specialized SOC**
Certain SOC are extremely specialized. They may wish to safeguard a particular piece of critical infrastructure. From classified sources, intelligence and knowledge about threats are collected. They employ security specialists, for example, to safeguard industrial control systems (ICS) and supervisory control and data acquisition systems (SCADA).

Framework

When developing a SOC, it is important to bear in mind that both external and internal criteria must be met. Conforming to a certain number of frameworks or certifications can increase an MSSP's marketability. Grobler, Jacobs, and Niekerk [11], suggest a range of relevant structures and standards for guiding and directing the development of SOCs. To resolve the full range of SOC requirements, it is also recommended to employ a combination of the following frameworks:

i. **ITIL**
ITIL (Information Technology Infrastructure Library) is an acronym for Information Technology Infrastructure Library. OGC is the issuer. While ITIL is very similar to CoBIT in several respects, the difference is that ITIL establishes standards from an organizational ICT perspective, while CoBIT establishes standards from a process-based and risk-based perspective.

ii. **CoBIT 5**
Control Objective over Information and Related Technology is the abbreviation. CoBIT is published by the Information System Control Association (ISACA), a not-for-profit organization dedicated to information technology governance. Its primary purpose is to assist organizations in mapping their information technology processes to ISACA best practices. Through implementing these activities, the enterprise's information and associated technologies can be regulated and handled holistically.

iii. **ISO/IEC 27001:2013 and ISO/IEC 27002:2013**
Both are security standards that apply to information systems. The ISO Board is the framework's issuer. They cover a smaller but more comprehensive domain than ITIL and CoBIT.

Both requirements enable an agency to be audited formally for enforcement by an independent and certified body.

Security

Security domain definitions, structures, and models are used to ensure a stable environment for SOC implementation. The following requirements are critical: information security policy, procedure, procedures, technology, security models, data protection, and staff security.

Policy, Procedure and Process

- According to the NIST Computer Security Incident Handling Guide [18], it suggest the following organizational structure for the security incident handling process:
- Create a protocol, a strategy, and procedures for incident response.
- Prepare incident reports with the required agency.
- Develop protocols for communicating with other parties about security incidents.
- Relevant personnel should be recruited and trained
- Determine which other groups within the company will be required to participate in certain aspects of the process.
- Determine the types of services they can provide

According to Torres [7], the DOE/CIAC model is a commonly used incident response process model, and it consists of six stages: preparation, identification, containment, eradication, recovery, and lessons learned. The model helps to standardize SOC analysts' behavior and ensures that no important tasks are ignored during the process. The functions and tasks of team members are defined by implementing a repeatable incident management procedure, from alert generation and initial Level 1 assessment to escalation to Level 2 or Level 3 personnel. It also allows for efficient resource distribution.

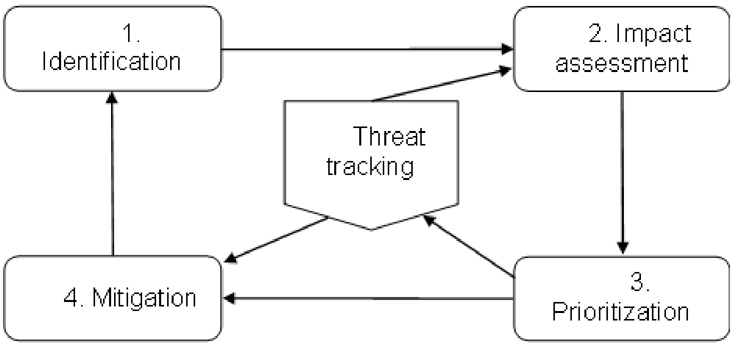


Figure 4: Process of Threat Mitigation and Management

Identifying threats by event reporting is the first step in the threat mitigation and management process. The probability, expense, timetable, technological efficiency, and capability of identified events are all evaluated. When an accident is upgraded to an incident, it is classified as a hazard. Second, the threat's effect is evaluated. Thirdly, risks would be prioritized and analyzed. For threats with a medium to high level of criticality, incidents will be constantly monitored and, if necessary, transferred to the incident management team. Low-level risks can be monitored further. The final and final move is threat reduction. This move involves incident management and ongoing monitoring to ensure that the company is aware of the status of threats [11].

Technical

The aim of the technical domain is for the SOC to have the appropriate facilities, technologies, policies, and procedures in place to provide cyber security monitoring, detection, and response services.

4.3. Architecture

Data collection, data processing, correlation analysis, and visualization are the four key components of SOC architecture design [19]. Figure 5 depicts the architecture model.

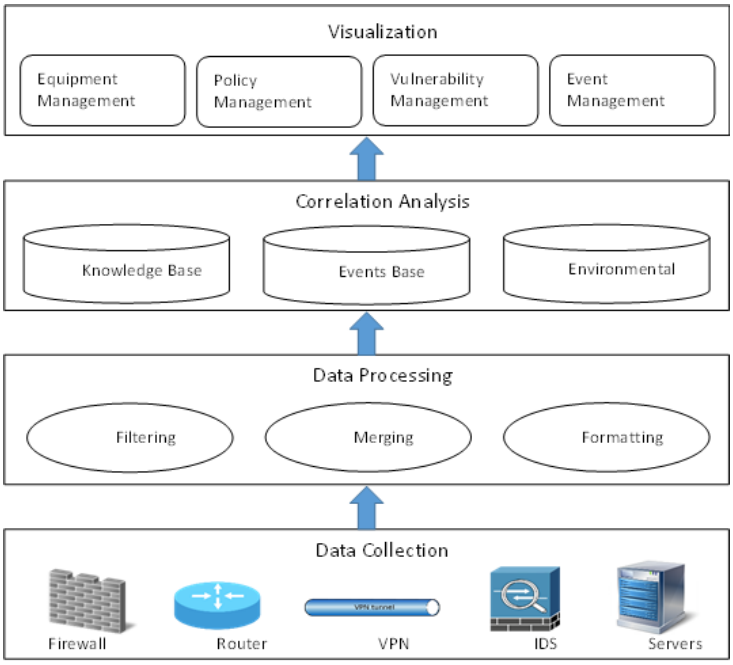


Figure 5: The architecture of SOC

Each unit carries out the following functions:

i. **Data Collection**
Data collect from security devices such as VPNs, firewalls, routers, intrusion detection systems, and servers. Data is collected in the form of asset logs and security incidents. These data are collected via Simple Network Management Protocol (SNMP) and SYSLOG.

ii. **Data Processing**
This unit is comprised of three main processes: data filtering, data merging, and data formatting. The first method eliminates redundant data, eliminates superfluous data, and reduces the large number of events. As a result, it becomes easier to locate the necessary data. Data merging is the process of combining several related pieces of data according to predefined laws. Similarly, would minimise the number of duplicated incidents. The data format converts disparate types of data into a cohesive body.

iii. **Correlation Analysis**
Correlation analysis is used to identify possible risks, prevent false and duplicated data, produce valid incidents, and optimise the network's performance and protection. Correlation rules are used to identify various types of attacks across the network, and these rules are customized to the user's specifications.

iv. **Visualization**
Visualize the findings of the network's security assessment.

Technology Selection

The fundamental technology SOC must achieve includes data collection, aggregation, detection, management, and analytical solutions [7]. SOC requires continuous data collection from various data sources to foster a more efficient security monitoring framework (Refer figure 6). It is important to remember that data silos in every company are adverse and prevent cooperation on security monitoring in their life. Furthermore, the capacity of an incident- and before-incident tracking system that collects data allows the safety analysts to use the system rather than a detection tool. The compatibility of the selected technology is also significant.

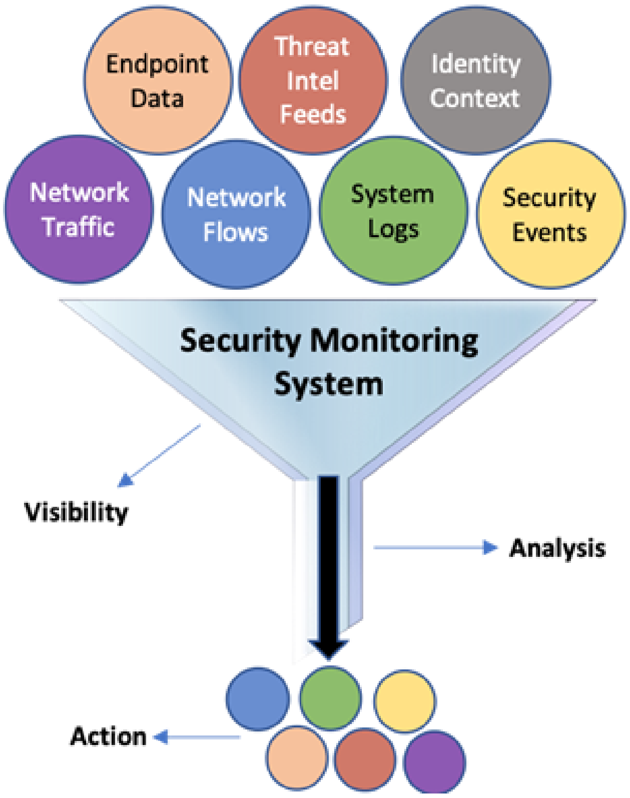


Figure 6: Data Aggregation. Reprinted from "Building a World-Class Security Operations Centre: A Road Map", by Alissa T, 2015

The Author emphasises the following criteria/capabilities in technology selection:

i. Visibility

ii. Get an insight into the danger by potential anomalies.

iii. Analysis enables SOC analysts to analyse large volumes of incident data and triage equipment.

iv. Actuations: Automatically adjust, manually or both. Patching, modifying firewalls, quarantining method, invalidating a certain certificate, for example.

Tool Selection
This section describes tool selection for SOC [13].

i. **Software**
Constructed with server software installed. The SOC will benefit from the deployment of several servers where it can be used for further tasks.

ii. **Hardware**
Built around servers with SOC software enabled. It is easier to deploy this solution. However, since the environment is isolated, no more applications can be added.

iii. **Infrastructure Solution**
SOC is a prepared, tool-based solution. The ability to normalize, aggregate and correlate using the database and queries is carried out. A comparatively lower cost and greater flexibility are the advantages of implementing this approach. The need for technical personnel to increase SOC capabilities gradually, however, is one downside.

Security event is also unusual in most companies today. Many security professionals manually perform log checks and for others the simple SIEM framework implementation is a minimum. About the SIEM scheme, the analysis [20] suggested grouping selection criteria into two categories:

i. **Functional criteria**
To decide whether the SIEM tool will accomplish what it should. Collection of logs, standardization of incidents, correlation and warning management is the key feature.

ii. **Technical criteria**

- **Vendor:** The choice of the supplier is dependent on several factors including quality and price ratios, the popularity of the supplier, quality, operation, information security expertise, engagement in research and development and its independence from other suppliers.

- **Integration:** Find the compatibility and data processing and normalization of the product for all operating requirements.

- **Ease of deployment**

Evolution of the product: To maintain high functionality and therefore satisfy the requirements of companies, the evolution of the state of the chosen product must be considered. You can easily obtain a new version of the goods with patch updates.

The author noted however that one organization could not possibly provide the best SIEM system for a particular organization, thus emphasizing that each organization should conduct its own assessment to choose the best system for its setting.

Operations

Cyber security practices such as protecting a portion of the cyber space and monitoring and analyzing threats and events, as well as responsive and proactive defense from emerging threats, are examples of cyber security practices.as well as management and recovery from incidents, have been described by Kowtha, Nolan and Daley [4] as activities. Near communication between SOCs is important to protect the cyberspace. For example, it is useful for one company to support one another with tactics, strategies and procedures used by malignant sources, identified and deduced. As shown in Figure 7, SOC requires a CISO and CIO governing body.

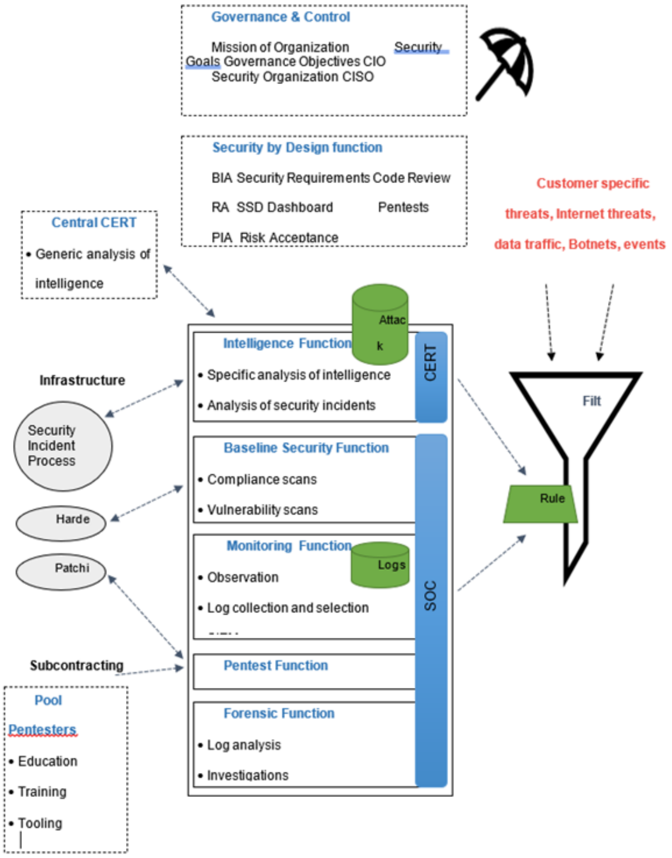


Figure 7: Technical Operation Flow of a SOC

The five-core feature 'Identify,' 'Protect,' 'Detect,' 'React' and 'Recover' is defined in the NIST cybersecurity framework. Those five functions serve as the primary pillar in carrying out cybersecurity projects. They help organizations portray their cybersecurity risk management at a high level and help them The role 'Safety by Design' ensures the safe development of service. They ensure that the manufacturing environment is passed on only with the safe solution. The business impact analysis, risk analyse and data protection analysis are another phase that has taken place in this function [9]. Intelligence, basic safety, surveillance, pen testing and risk management decisions are the other five areas [21]. In scholarly writing, information on functionality was widely discussed. The NGSOC system must comply with the cyber security framework because of its value. The table 6 underlines the heatmap of the instruments used by SOCs which meet five NIST Cybersecurity Framework functions:

Identify

The identification role can be seen as the basis for an organisation's overall security position. It calls upon organisations to better consider the cyber-safety threats associated with them and how to handle them properly. The identification role ensures that the defensive function does not neglect major properties. With the the use of IoT devices and networks, the information security team faces challenges to manage such an immense number and activities and sources of security incidents [13].

Defining normal by baselining is a technology that allows incidents to be distinguished from normal and suspicious or non-standard behaviours. Any analysts in Tier 1 should be notified with actionable alerting systems equipped with the right baselining technique. These notifications are prioritised automatically and simplify an analyst's job. The best practise is to enforce basic standards for the determination of the usual status and to set the event thresholds in a security monitoring platform for a long time. If an irregular event is detected by the device, the platform should warn of the action needed [7]. The lack of such a baseline technique in their security control system is one capability most organisations are still to achieve, according to the SANS log management survey 2014 [22]. **Protect**

The Protect Role calls for stakeholders to be informed and apply adequate protections to protect the data and critical framework at the risk of cyber security occurrences. It is their task to exploit the organisational safety best practises that may include restricting and monitoring protected access to both physical and digital networks, applications and devices and providing safeguards against unauthorised access to these systems. Three critical protective pillar activities that help SOCs are identified in literature review [9].

i. Baseline Security

   - Reduce the surface vulnerability: Server, OS and network component hardening.
   - Security of implementation: anti-virus, firewalls, IDS/IPS, PKI.
   - Ensure the instructions are followed: Carries out compliance scans and weakness.

ii. Monitoring To detect abnormalities in network traffic, device logs, endpoint data and many other data sources SOC perform continuous supervision services. SOC A series of rulebooks for dynamic correlation are used for the retenue of large volumes of log data in order to identify and detect the legitimate threat from all logs that are received. Since the driving force for cyber-attacks is a changing state and cyber criminals continually improve their strategies, security professionals must remain aware of the current threat environment. Therefore, it is an important challenge in SOC monitoring to change the SIEM settings to detect important events promptly.

iii. Penetration Test Entry tests can assess the reaction of the system to an attack, the intensity and the knowledge that the system can obtain from it, as well as its protections against potential failures.

Detect

The role detect is to develop and enforce a number of activities which recognise cybersecurity events and allow cybersecurity events to be detected in good time. The relationship (dependency between SOC entities) technology plays an important role in the process of event detection. The previous research describes 7 correlation techniques defined as follows [13].

Table 3: Staff Duties and Training Needs. Adapted from "Building a World-Class Security Operations Centre: A Roadmap", by A. Torres, 2015, SANS Institute.

Job Title	Duties & Responsibilities	Training/Certification
Tier 1 Alert Analyst	• Continuously monitors the alert queue • Conduct security alert prioritization • Monitor's health of security sensors and endpoints • Collects data required to initiate task for Tier 2	• Alert triage procedures • Intrusion detection • SIEM • Host-based investigation • SANS SEC401: Security Essentials Bootcamp Style
Tier 2 Incident Responder	• Performs thorough incident analysis by correlating data from various sources • Determines if a critical system or data set has been affected • Advises on rectification • 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 • Threat intelligence • 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	• Look for incident, rather than waiting for escalated incidents • Involves in development, implementation, and fine tuning of threat detection analytics	• Advanced training on anomalies detection • Tool-specific training for data aggregation, analysis, and threat intelligence • SANS SEC503: Intrusion Detection In-Depth • SANS SEC504: Hacker, Tools, Techniques, Exploits and Incident Handling • SANS SEC561: Intense Hands-on Pen Testing • SANS FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
SOC Manager	• Manages resources (personnel, budget, shift scheduling, technology strategy) to meet SLAs • Communicates with management • In-charge for business-critical incidents • Provides overall direction for the SOC and input to the overall security strategy	Project management Incident response management General people management CISSP CISA CISM CGEIT

Table 4: Counteraction Capabilities

Counteraction capabilities	SOC without counteraction capabilities	Reactionary SOC
Description	SOC is using IDS. It tracks and visualizes security incidents and prioritizes them. If an attack is observed, no response measures are taken. SOC's main aim is to process data, visualize events and comply with regulations.	Instead of detection of attack, preventive measures are taken to stop the attack from SOC apply the IPS principle. The automatic mitigation feature provides rapid response to IS threats.
Environment (E.g., banking)	High demands for availability	High demands for confidentiality
	High availability requirements	High levels of confidentiality are required (E.g., banking)
	Requirements for high availability	
Tools	Open System Software, Netforensics, and the eTrust Security Information CA Management Solution	Check Point Eventia Analyzer, IBM Tivoli Security Operation Manager Software, and Cisco Monitoring Analysis and Response System

Table 5: Deployment Scenarios.

Deployment Scenarios	Centralized	Distributed
Description	SOCs are deployed on a single device/server that handles all aspects of information security management.	Multiple devices/servers are being deployed. The load balancing between them takes place simultaneously.
Advantages	Greater speed, ease of installation and relatively low cost.	Better performance and overall effective SOC.
Drawbacks	Greater pace, easier assembly, and low cost. Suitable for small to medium sized environments only.	Due to multiple devices used, costs are greater, and deployment and maintenance is more complex.

Table 6: Heatmap of tools used by SOC in regard to NIST Cybersecurity Framework.

Functionality	Identify	Protect	Detect	Respond	Recover
Intrusion Detection System (IDS)	✓	✓	✓		
Intrusion Protection System (IPS)	✓	✓	✓		
Log management	✓	✓	✓		
Access Control		✓			
Vulnerability Management		✓			
Penetration Testing		✓			
Endpoint Monitoring and Logging		✓			
SIEM	✓	✓	✓		
Windows Event Log Monitoring	✓		✓		
Risk Analytic	✓		✓		
Threat Intelligence	✓	✓	✓		
Asset Management		✓			
Continuous Vulnerability Assessment		✓			
Web proxy		✓			
Application Log Monitoring	✓		✓		
Packet Analysis	✓		✓		
DNS Log Monitoring	✓		✓		
DoS/DDoS Protection	✓	✓	✓		
Malware Protection		✓			
NextGen Firewall		✓			
Web Application Firewall (WAF)	✓	✓	✓		
Data Loss Prevention		✓			
Inline Malware Destruction		✓			
Application Whitelisting		✓			
Endpoint Detection & Response	✓		✓	✓	
Egress Filtering	✓		✓		
NetFlow Analysis	✓		✓		
Threat Hunting	✓		✓		
Encrypted Traffic Inspection	✓		✓		
eDiscovery	✓		✓		
Network Analysis	✓		✓		
Deception Technologies	✓	✓	✓	✓	
Machine Learning	✓		✓		
Network Forensic Analysis				✓	✓
Host-based Forensic Analysis				✓	✓
Adversary Containment				✓	
Command Centre				✓	
Customer interaction (call centre)				✓	
Playbook-based response actions				✓	
Workflow-based remediation				✓	
Constituent Communications				✓	
Adversary Interruption				✓	
Threat Neutralization				✓	
Reverse Engineering of Malware				✓	
Public Relations Coordination				✓	
Threat Attribution				✓	
Threat Campaign Tracking				✓	
Adversary Deception				✓	
Hardware reverse engineering				✓	

Table 7: Correlation techniques

Techniques	Benefits	Drawbacks
i. Statistical Based on its existence and trends, SOC monitors network activity and detects threats. Then, statistical algorithms are used to calculate the severity of the incident to assign the value of the risk.	• Do not need to know precise trends of threats. • Does not include rules or substantial baseline definition. • Enables efficiency assessment	-
ii. Rule-based To recognise potential attacks, SOC employs predefined rules which apply conditional logic. Rules may be developed by vendors or based on due careful monitoring of traffic in networks.	Special security threats based on known patterns of attack are very successful.	• Updating all rules will take time. • Far from being adequately maintained about false positives and wrong negatives.
iii. Vulnerability Correlates network IDS security incidents against an established vulnerability database.Vulnerability profiles are collected, returning score for each asset.	• Special attack scenario detection and elimination of false positives is highly effective. • maximizing detection efficiency.	Intense labor to rule Creating specific vulnerabilities requiring rule creation.
iv. SLA SOC blends safety incidents with SLA needs. Models for business processes are focused on various safety incidents	Helps to estimate the network or elements deprived of service deficiency.	Composition and cost determination difficulties in business processes.
v. Compliance SOC combines the rule, the procedure, and the requirements of security accidents.	-	Need special configuration and configuration as the policies of any IoTI.
vi. Mixed All types of correlation techniques are applied.	Improved identification of attacks as well as improved management of the security of information.	-
vii. SOC without correlation SOC is capable of aggregating data, but the security personnel determine all other procedures.	-	Suitable for small networks only.

One of the underlying limitations is the bottlenecks of the response mechanism, given so much attention on the technologies for detecting threats. There are an overwhelming number of warnings every day that safety analysts are in 'alert fatigue.' Manual processes, capability shortages, and technology inclusion disparities are another issue facing SOC [7].

Respond

The 'response' feature allows stakeholders to take appropriate measures during a cyber security incident detection scenario. The 'reply' feature ensures the proper response planning, contact to stakeholders, cybersecurity incident analysis, detection of threats and changes in SOC's efforts under 'identify,' 'protect,' and' detect functions. CIAC is a model of an incident response procedure that exists since 1989 in the United States Department of Energy's Computer Incident Advisory Capacity (CIAC). The model identified six phases: planning, identifying, containing, eradicating, recovering and learning [7]. Special Publication 800-61 Review 2 proposes that incident response plan organisations should have a formal, targeted, and structured approach [18]. The plan should develop the requisite resources and management support, such as the task, objectives, and priorities, as well as senior management approval and an organizational approach to incident response.

Recover

The recovery role recognizes, develops and performs necessary activities to guarantee stability and restoration of any capabilities or services impacted by cyber safety. The position aids in the rapid restoration of normal operations in order to mitigate the effects of a cybersecurity incident. Part of ISIMP is to learn about safety incidents and provide preventive controls, and progress over time on overall incident management. ISIMP Incident Management [13].

During the retrieval procedure, administrators can retrieve systems in their usual operating state, check that systems operate normally and, where appropriate, remedy vulnerabilities in the future to avoid similar events. Recovery can include activities such as clean backup systems, scratch reconstruction systems and files replacement with clean copies, patches installation, password change, and network network perimeter protection tightening (e.g., firewall rules and the access control list on the border router) [18]. The remediation role consists of three parts as following in accordance with best practises or recommended standards, like ISO/IEC 27001:2013 [5]:

i. **Recovery planning**
The incidents shall be answered in accordance with the documented process in the event of incidents of protection of information.

ii. **Improvements**
To minimize the risk or effect of potential events, knowledge gained from the analysis and resolution of information security incidents is utilized.

iii. **Communications**
Public relations are managed, and reputations are restored and rehabilitation efforts conveyed both to internal and external stakeholders and to managers.

Intelligence

The knowledge feature lies at the heart of the SOC. In reality, with a computer emergency response team they share the same characteristics (CERT). Here, experienced and qualified security analysts share information with both internal and external parties. Among other tasks, they analyse trends of threats, track results, define rules on event filters and offer SOC personnel guidance [9]. They continue to improve their ability to process more data and maximize their ability to use intelligence threat to a fully developed SOC. Intelligence sources can also come from historical events, business partners, the law enforcement cybercrimes division or threat intelligence providers [7]. [11] discusses three intelligence which, depending on their audiences and implementation, involves the classification of intelligence into four separate levels.

Table 8: Levels of intelligence [11]

	Strategic	Operational	Tactical	Technical
Audience	• Board • Executives • Government	• Defenders • Senior security management • Analysts	• Analysts • Senior security management • Architects • System admins	• Analysts • Incident response • Security devices
Time-frame	Long-term	Short-term	Long-term	Immediate
Scope	General	• Industry sector • Community	Organization	Organization
Focus	• Political • Social • Economic • Behavioral	• Adversary campaigns • Specific incoming attacks	Attacker tactics, techniques and procedures	Indicators of compromise

Table 9: Sources of intelligence

Internal	External
• Network and security devices and applications • Servers and endpoints machine system logs • Application logs • Packet capture and inspection • Users and application behavior • Configuration, vulnerability, and compliance data	• Subscription of free commercial cyber threat intelligence feeds • Community shared threat and vulnerabilities information • Vendor supplied threat and vulnerability information • Social media and paste sites • Alerts from government intelligence and national CSIRTs

Outside sources provide proactive detection and identification capabilities for intelligence, in addition to internally gathering intelligence.A common misunderstanding is that signature feeds and compromise indicators are confused with intelligence. In fact, they make up the whole picture of intelligence.

Literature Analysis

The findings lack academic debate and arguments in the security and technical sector. The research gap will be filled by further investigations into this topic. In terms of similarity, the significance of individuals, processes, and technologies for building a SOC is recognised in all studies. The drive, configuration, operation, and technology used for each SOC model are different. The stakeholder and functionality within SOC are a strength that can be highlighted and that is well defined. There are also many drawbacks, for example: Due to the singularity of the source, it is impossible to compare results. There is a lack of adequate, accurate documentation for building SOCs, and literature focuses mostly on technical aspects.

The table below shows the availability of relevant knowledge in each source of literature:

Table 10: Literature Analysis

	Citation	[8]	[13]	[9]	[7]	[4]	[11]	[14]	[17]	[19]	[20]	[16]
Stakeholder	Stakeholder requirement	Yes	Yes	Yes		Yes	Yes					
	Service Management	Yes	Yes					Yes				
	NGSOC Management	Yes	Yes			Yes	Yes					
	Stakeholder reporting							Yes				
	Facilities Management											
	People Management			Yes	Yes				Yes			Yes
	Operational Management		Yes	Yes								
	Framework						Yes					
Security	Policy, procedure, process				Yes		Yes					
	Physical Security											
	Technical Security											
	Data Security											
	People Security											
Technical	Architecture									Yes		
	Technology Selection				Yes							
	Tool Selection		Yes	Yes							Yes	
	Operations			Yes		Yes						
	Identify	Yes	Yes		Yes							
	Protect	Yes		Yes								
	Detect	Yes	Yes		Yes							
	Response	Yes			Yes							
	Recover		Yes									
	Threat Intelligence			Yes	Yes		Yes					

5. Future work

Several preliminary research questions concerning the portion of the NGSOC framework remain unanswered based on the detailed findings of previous related work. Table 7 outlines the functional requirements needed for integrating individuals, processes, and technologies. There are no proper standards an organization should behave in line with when it comes to physical safety, personal protection, data security and operational architecture. These building blocks not only cover a center's technology and process aspects but also the human element as stakeholder, governance, and safety. It is anticipated that the company can eventually minimize its cyber risks to an appropriate level by defining criteria for each field.

Table 11: NGSOC Framework (High-Level)

Building Blocks	Domain	Functional Requirement	Services
People, Process, Technology	Stakeholder	Stakeholder Requirements	Real-time Log Monitoring, Intrusion Detection, Incident Handling, Incident Response, Vulnerability Assessment, Penetration Test, Threat Analysis, Threat Intelligence, Network Forensic, Security Awareness Training.
		Contract Management	
		Service Management	
		NGSOC Management	
		Stakeholder Reporting	
	Governance	Facilities Management	
		People Management	
		Operational Management	
		Framework	
	Security	Policy, Procedure & Process	
	Technical	Architecture	
		Technology Selection	
		Tool Selection	
		Operations	
	Functionality	Identify	
		Protect	
		Detect	
		Respond	
		Recover	
	Intelligence	Threat Intelligence	

To meet the needs of these researchers, the NGSOC system was developed to help organizations disclose accurate and valuable information on the efficacy of their risk management cyber security programs. SOC must go beyond surveillance and assist with a swift and successful response to cyber security incidents. The study results will be a major component of the enterprise-wide risk management program for cyber security organizations. This knowledge will enhance an awareness of the global security position of companies and allow analysts, executive directors, investors, and business partners to manage risks.

6. Conclusion

Since then, the cyber threat has led to a huge loss in terms of consumer loyalty, security, confidentiality, credibility, and accessibility for many organizations, in the Industrial Internet of Things (IIoT). To initiate a cyber-attack is progressed, organizations need a more proactive strategy for detecting and retrieving potential events. The results of the research would allow any organization to create their own software, while mitigating the impact of cyber-attacks, to improve the NGSOC framework for a future analysis. For future work, the SIEM system engine is used to model a threat to real life by designing some correlation rules that will be integrated into the system.

7. Acknowledgment

This work was supported by SysArmy Sdn. Bhd and Faculty of Computing, University Malaysia Pahang (UIC190807).

References

[1] A. Torres, *Building a world-class security operations center: A roadmap,* https://sibertor.com/wp-content/uploads/2016/07/building-world-class-security-operations-center-roadmap-35907.pdf.

[2] Bank Negara Malaysia, *Risk Management in Technology (RMiT),* 2018.

[3] C. Crowley, *Future SOC: SANS 2017 Security Operations Center Survey,* 2017.

[4] C. Onwubiko, *Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy,* Int. Conf. Cyber Sit. Awar. Data Anal. Asses. 2015.

[5] F. D. Janos and N. H. P. Dai, *Security concerns towards security operations centers,* SACI 2018-IEEE 12th International Symposium on Applied Computational Intelligence and Informatics, Proceedings, (2018) 273–278.

[6] Frost & Sullivan, *The 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk,"* Frost & Sullivan in partnership with Booz Allen Hamilton for ISC2, (2017) 1–8.

[7] ISACA, *COBIT 5: An Introduction,* 2012.

[8] ISO/IEC, *Information Technology – Security Techniques – Information Security Management Systems – Requirements (ISO/IEC 27001:2013),* 2013.

[9] J. Shenk, *Ninth Log Management Survey Report,* 2014.

[10] M. Grobler, P. Jacobs and B. van Niekerk, *Cyber security centres for threat detection and mitigation,* Threat Mit. Det. Cyber Warf. Terr. Act. (2014) 21–51.

[11] M. Nabil, S. Soukainat, A. Lakbabi and O. Ghizlane, *SIEM selection criteria for an efficient contextual security,* Int. Symp. Networks, Comput. Comm. (2017) 1–6

[12] M. Townsend, *How a crippling shortage of analysts let the London Bridge attackers through,* 2017.

[13] NetIQ, *Service Level Agreement Guide,* 2016.

[14] NIST, *Cybersecurity Framework's Five Functions,* (2018)

[15] N. Miloslavskaya, *Security operations centers for information security incident management,* Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud (2016) 131–138.

[16] P. A. Networks, *Build a Next-Generation SOC Techbrief,* 2011.

[17] P. Cichonski, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology,* NIST Special Pub. 79 (2012) 800–861.

[18] S. Bhatt, P. K. Manadhata, and L. Zomlot, *The operational role of security information and event management systems,* IEEE Security and Privacy, 12(5) (2014) 35–41.

[19] S. Kowtha, L. A. Nolan and R. A. Daley, *Cyber security operations center characterization model and analysis,* IEEE International Conference on Technologies for Homeland Security, HST, (2012) 470–475.

[20] S. Schinagl, K. Schoon and R. Paans, *A framework for designing a security operations centre (SOC),* Proc. Annual Hawaii Int. Conf. Sys. Sci. (2015) 2253–2262.

[21] S. Yuan and C. Zou, *The security operations center based on correlation analysis,* IEEE 3rd Int. Conf. Comm. Soft. Netw. (2011) 334–337.

[22] Symantec, *Internet Security Threat Report,* 2017.