Planning the Building a SOC: A Conceptual Process Model

Pierre Jacobs[1], Sebastiaan von Solms[1] and van der Walt[2]
[1]University of Johannesburg, South Africa
[2]Sizwe IT Group – South Africa
pierrej06@gmail.com
basievs@uj.ac.za
svdwalt@gmail.com

Abstract: There are few frameworks available to consult when building Security Operation Centers (SOCs). (P. Jacobs, 2015). Jacobs proposed such a framework, and this paper builds on the "Planning" part of that framework. The authors could not find any existing conceptual process models where it comes to the planning phase when building SOCs. We propose a conceptual process model to follow during the planning phase of the SOC. Conceptual models are used to represent systems typically made up of the composition of concepts (Robinson; Arbez; Birta; Tolk; Wagner, 2015). The aim of our conceptual process model is to help SOC builders understand the proposed process to be followed during the SOC planning phase and is meant to guide the SOC builder's thinking during the planning phase. The conceptual process model will start by determining the services that the SOC in development will be offering, followed by deciding on a SOC model. After the determination of the SOC services and model we will identify the technologies and tools to facilitate the services, keeping in consideration the influence the SOC model has on the service. For each of the steps in our conceptual model we have identified existing, public frameworks, standards or best practices. Our conceptual process model will be mapped to these frameworks, standards or best practices with the intention to be used to augment our model.

Keywords: SOC planning, SOC conceptual process model, SOC services, SOC models, systems engineering, SOC builder, MSSP, EDR, MDR

1. Introduction

Cybersecurity is a topic being discussed globally by executives. In todays connected world, the protection of cyber assets is of extreme importance. There are many reasons for considering cybersecurity – some of these are the protection of organisational sensitive information, ensuring availability and integrity of cyber resources, as well as to comply with legislative and internal governance requirements. Information technology is a key enabler in today's business world, and it should be protected like any other asset in the organisation. Therefore, it is important for any company to have a Cyber Security Strategy.

A good, solid cyber security strategy will benefit business in the following ways as taken from (The British Standards Institution, 2014):

- Protect networks, computers and data from unauthorized access
- Improved information security and business continuity management
- Improved stakeholder confidence in your information security arrangements
- Improved company credentials with the correct security controls in place
- Faster recovery times in the event of disruption

Furthermore, important outcomes which can be expected when a Cyber Security Strategy is supported by an effective governance approach, is reduced cyber risk, and reducing potential business impact to an acceptable level. Such a governance approach allows for the strategic alignment of security with the enterprise strategy and organisational objectives. Market share could also potentially be preserved and increased due to the reputation for safeguarding of information, and lastly, security investments are efficiently utilised to support organisational objectives.

In achieving such governance goals, technical and administrative controls are used. The function of the deployed technical controls varies widely – some protect against unauthorised access, and loss of data, to intrusion and malware detection and prevention on the network, and endpoints. Furthermore, these technical controls need to be monitored to ensure that they function as intended, and that they are configured correctly.

Some of these technical controls such as firewalls, Intrusion Prevention Systems (IPS) and anti-malware software are used to monitor for events with the aim to detect possible attacks, breaches, and compromises, and to

perform specified actions to react to these attacks such as containing or blocking them. These technical actions are supported by a solid incident response capability offered from the SOC. We will in Section 2 propose a definition for a SOC.

2. Background - What is a SOC?

Experience showed that a SOC can be defined as a single, central repository where logs from multiple sources are collected, aggregated, and correlated. The log events are monitored and investigated and elevated into incidents if needed. These incidents are then escalated internally or to clients and then responded to by the relevant teams depending on the incident at hand. Response could be in the form of remediation or containment. A SOC is made up of people, processes and technologies (Logsign, 2018)(McAfee, 2021).

When planning on consuming or using SOC services, there are two different choices open to organisations (Digital Hands, 2021); (Dave Young, 2020). The first choice is to build their own SOC (organisational SOC – also called an in-house SOC, or insourced SOC). The second choice is to consume SOC services from a Managed Security Service Provider (MSSP – also called an outsourced SOC). From a services perspective MSSPs cater for multiple clients from different industries and they are externally focussed in that they look after the interests of customers. Organisational SOCs looks after the interests of a single organisation, and they are internally focussed in that they look after the interested of the organisation they serve.

There are thus two distinct types of SOCs with different operational requirements and approaches, but from a technology perspective they would both use the same tools, The primary tools used to monitor for and respond to incidents are the Security Incident and Event Monitoring (SIEM) and Security Orchestration, Automation and Response (SOAR) tools. The two SOC types are shown in Figure 1. Our conceptual process model was developed to cater for both organisational SOCs and MSSP SOCs. Taking the above into consideration, we will use the term "*SOC"* as an umbrella term to describe both organisational SOCs and MSSPs.

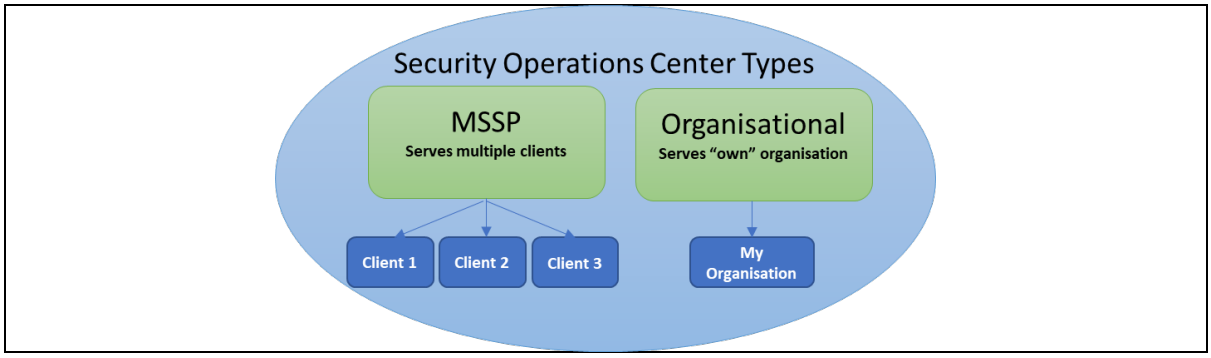

Figure 1: SOC types

The authors could not find any conceptual process model describing the higher-level planning steps when planning to build a SOC. In this paper we propose a SOC conceptual planning process model that describe the higher-level steps to follow when planning to build a SOC. This conceptual process model should be used first before a detailed "Build Framework" such as the one described by *Jacobs* (2015) (P. Jacobs, 2015) is used.

In Section 3 we introduce a methodology to identify SOC services. In Section 4 we identify SOC services and in Section 5 we introduce the different SOC models. In Section 6 we will map the SOC services to technologies and in Section 7 we follow a systems engineering approach to identify the most suitable SOC technologies. The planning steps in our model is mapped back to existing, public frameworks, standards and best practices in Section 8.

3. An introduction to our conceptual process model to plan for SOC building

When planning and building a SOC, experience showed that it is beneficial to follow a structured approach (such as a framework) to ensure that all people, processes and technology aspects are considered. An example of such a framework is the one proposed by Jacobs (P. Jacobs, 2015). Experience showed that the choices made during the planning phase influences the technology requirements as well as the number of resources (people) and the skills they need to have. At a high level, we propose the following six steps to guide and focus the SOC builder's planning and thinking.

- **Step 1:** Define the services to be offered by the SOC – services are supported by people, processes and technologies. Services definitions are normally defined during structured interviews with stakeholders.
- **Step 2:** Determine the SOC model – the SOC model further influences the number of resources needed. It also influences facility requirements as well as legal and regulatory requirements.
- **Step 3:** Identify and map technologies to facilitate and support SOC services.
- **Step 4:** Select technologies such as SIEM and SOAR platforms (see Paragraph 5.1). This should be done by soliciting user requirements, draft functional and technical specifications and issuing a Request for Proposal (RFP).
- **Step 5:** Plan Facility and Infrastructure. This is the building, the physical security and the screens, seats and desks and communications infrastructure needed to make the SOC work.
- **Step 6:** Identify people requirements (skills and experience) and develop SOC operational processes to support SOC services.

After the SOC services and SOC models are defined, the facilities and infrastructure are built, resources recruited, and technology procured. Once all this is done, processes, procedures, use cases and playbooks are developed. The six steps of the high-level conceptual process model are shown in Figure 2.

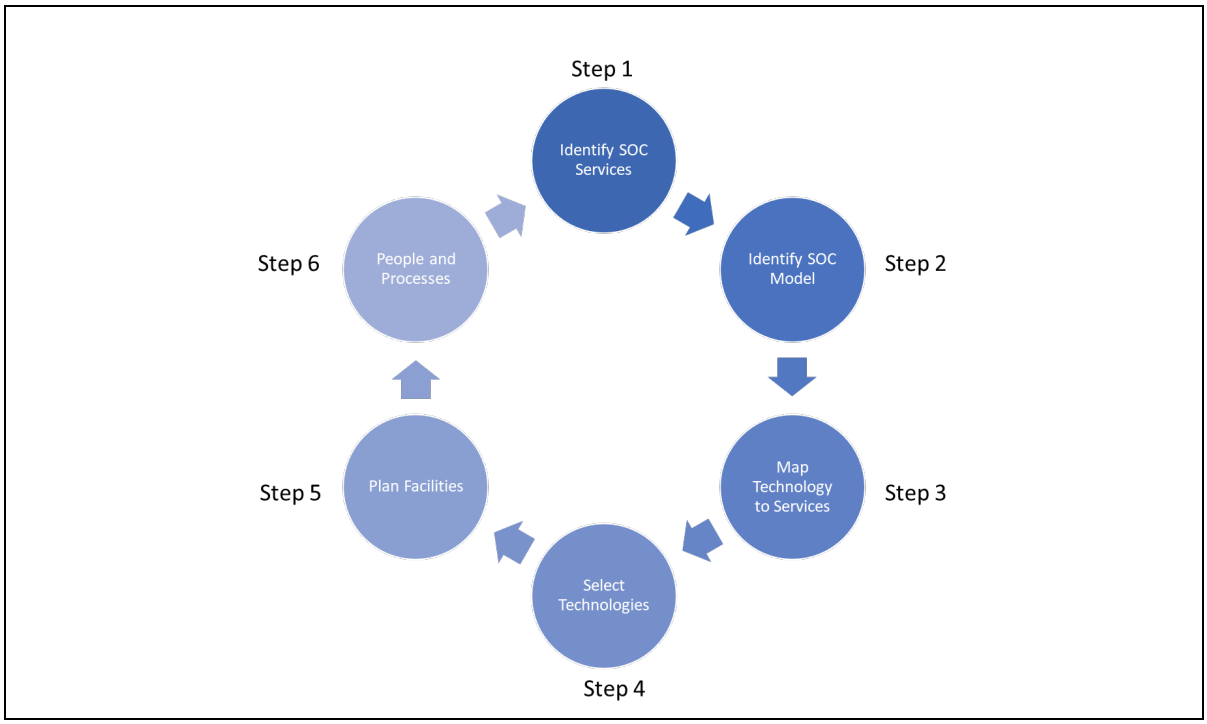

Figure 2: SOC builder conceptual process model

To illustrate the application of our conceptual process model we will describe Step 1 to Step 4. Steps 5 to 6, the planning for facilities and the planning for people and processes steps will be described in future work. We will now introduce Step 1 of our conceptual process model - the identification of SOC services, and a methodology to follow during their identification. Potential SOC services, and the methodology we have followed to discover them, are introduced in Section 4.

4. Step 1: Identify SOC services

It is our experience that some organisations follow a bottom-up approach in that they first procure tools and technology and then define the services around the technological capabilities. From an organisational SOC perspective this is the least desirable way to identify services as it will almost always be limited by technological constraints. MSSPs however may find this a useful way of identifying service offering to clients as they typically cater for multiple clients at a time.

For MSSPs functional capabilities such as multi-tenancy and role-based access may be important, while automated workflow and correlation capability may be more important in an organisational SOC. We will follow

a top-down approach by identifying the SOC services and models first, and then build the enabling technology stack around it.

The SOC services selection will influence the SOC tools and technology as well as its processes. It is our experience, and supported by literature (SANS Institute, 2021) that the services offered by MSSPs can be grouped into primary and secondary services. The SOC Builder may use five different methodologies to determine SOC primary and secondary services. Primary services are the core services offered by SOCs such as monitoring, detection response and threat intelligence. These are the most basic services that should be offered from a SOC. Secondary services are services such as device management and user awareness training. They are not core to the SOC but augments the SOC service basket. Primary services can be determined by observing the following five-step methodology described next.

- 1. Through Market research

Market research is done to determine what services clients require from SOCs. The market research can be a simple desktop research exercise or using a third party to do the market research on the SOC's behalf.

- 2. By Identify existing pre-defined SOC services

It is our experience that existing MSSPs will already have a basket of pre-defined services on offer to clients. SOC builders could leverage off this knowledge. This pre-supposes a good relationship between the upcoming SOC and other industry players. Jacobs *et al* (Jacobs *et al.*, 2016) identified and pre-defined a basket of SOC services that may be used by the upcoming SOC to select services from.

- 3. Through Structured interviews with industry and stakeholders

SOC service requirements are solicited during structured interviews with stakeholders. The advantage of following this approach is that the establishing SOC starts building relationships with potential clients and will get a solid understanding of stakeholder's service requirements and performance metrics.

- 4. By Services implied from authoritative and normative sources.

Authoritative and normative sources are consulted to identify potential SOC services. This approach has the advantage that establishing SOCs consider national and international requirements and prescriptions expressed in these sources. Sources could be national acts and regulations, or standards and frameworks used by industry and stakeholders.

- 5. Through a combination of the listed methodologies

Following a combination of all these methodologies will yield the best results in that stakeholders as well as national and international prescripts and requirements are consulted. This leads to a relevant and market related services definition.

Following our proposed five-step methodology and backed by experience, and supported by literature, the three primary services that should be offered by SOCs are (SANS Institute, 2021) (*SOC-as-a-Service, MDR, and Managed SIEM. What's the Difference? - MSSP Alert*, no date)(C. Zimmerman and Operations Center, 2014):

- **Monitoring** - this service describes the near real time analysis of data from telemetry sources for potential threats. This is mostly achieved using a SIEM.
- **Detection** - this describes "the action or process of identifying the presence of something concealed." (*Detection | Meaning of Detection by Lexico*, no date). This is mostly achieved using a SIEM or SOAR platform.
- **Response** - could be in the form of incident handling or facilitating the actual remediation. Response could be automated using a SOAR tool.

Where the detection and response services are managed, it is known in the industry as Managed Detection and Response (MDR). The MDR service can be delivered using the clients own set of tools, or by tools provided by the service provider (Zhang, 2018).

To make sure the primary and secondary services are offered in an effective and measurable way, service metrics and key performance indicators need to be identified, and processes supporting the service need to be developed and their effectiveness and maturity managed.

Now that we have introduced the idea of SOC services, we move to the identification of SOC models in Section 5.

5. Step 2: Identify SOC models

It is important to identify the available SOC models since the model influences the services, and thus the technology requirements. We identified two SOC types in Section 2. The types are an organisational SOC, and MSSP SOC. Both types offer or provide a service or services to clients. The organisational SOC provides a service to an internal client (its organisation) and a MSSP to external clients. SOC models can thus then be viewed from two contexts.

The first context is the consumer context. The consumer context views the SOC services from the internal or external client's perspective. Our experience showed that the consumer has five different operational requirements when looking for SOC services.

The second context is the service provider context (organisational SOC or MSSP perspective). This context describes how organisational SOCs or MSSPs structure their services operationally. We identified two different service provider operational models. We will now discuss these in more detail:

5.1 Consumer context

From experience, we identified five SOC operational models from a consumer context. These are:

- Monitoring detection, and response are performed internally (organisational SOC).
- Outsourced monitoring and detection (MSSP) with internal response (organisational SOC).
- Outsourced monitoring and detection with outsourced response (MSSP).
- Co-sourced monitoring and detection with internal response (organisational SOC and MSSP).
- Co-sourced monitoring and detection (organisational SOC and MSSP) with outsourced incident response (MSSP).

5.2 Service provider (MSSP) context

From experience we have identified two primary MSSP operational models. These are:

- SOC as a Service (SOCaaS) - this model describes the traditional MSSP SOC that provides monitoring detection and response services to clients. These capabilities are developed internally and are inherent to the MSSP model.
- Co-Sourced SOC - This model describes an MSSP SOC that outsources the delivery of some of its services to external entities (partners or clients). In some instances, responsibility to deliver a specific service may be shared, and these are typically described as part of the SOC playbooks i.e. where the SOC outsources threat intelligence or remedial efforts to a third-party service provider.

The two contexts from where SOCs can be viewed from, and the operational models are summarised in Table 1.

Table 1: SOC contexts and operational models

Context 1: Consumer Context	Context 2: Service Provider (MSSP) Context
[1]Internal monitoring, detection and response [2]Outsourced monitoring and detection with internal incident response [3]Outsourced monitoring and detection with outsourced response (MSSP) [4]Co-sourced monitoring and detection with internal incident response [5]Co-sourced monitoring and detection with outsourced incident response	[1] MSSP/ MDR [2]Co-Sourced MSSP / MDR

Now that we have identified the SOC primary services as well as the SOC operational models, we need to map the services and SOC models to technology requirements in Section 6. For illustrative purposes we will focus on the MSSP context.

6. Step 3: Mapping services to technology

The three primary SOC services that we have identified for both organisational SOCs and MSSP are the monitoring detection and response services (see Section 3). A service is made up of people, processes and technologies (P. Jacobs, 2015). The focus of this section is on the technologies needed for these primary services, and in context of MSSPs operational model we identified in Section 4.

6.1 Monitoring service

Hewlett Packard defines security monitoring as the collection of logs and analysing the information therein to detect possible threats and attacks. Security monitoring includes the capability to trigger alerts and action triggered alerts. The primary technology used to monitor for security related alerts are a SIEM tool (HPE, 2018).

This service presupposes that the client has security technical controls installed and that the logs from the security controls can are sent to the SIEM tool. The purpose of a SIEM is to collect many logs from different telemetry or log sources. These telemetry or log sources may be from perimeter and network controls, to end-point protection logs. These logs are parsed, in some cases aggregated, often correlated and algorithms are applied to identify incidents and events of significance (J. Miller, 2019). The SIEM capabilities are often supported by a SOAR.

A SOAR platform's primary function is to collect and organise information and present it in such a way that cybersecurity staff can easily manage and process the information. The aim is to standardise and incorporate incident investigation into existing workflows. Information is collected from a range of telemetry sources and this information is delivered to a central hub. A SOAR platform helps to automates incident response through the categorisation and classification of alerts, with the end goal of reducing the amount of alerts seen on SIEM (J. Miller, 2019).

6.2 Detection service

In context of a MSSP, this service could be offered using the client's own tools, or tools provided by the MSSP. When combined with the Response service, and offered by a MSSP, it is also sometimes referred to as Managed Detection and Response (MDR). MDR service offered by service providers, such as MSSP SOCs, share the same characteristics (Zhang, 2018).

The first characteristic of a MDR service offered by a MSSP is that MSSP's MDR service focus is on threat detection, and not so much on compliance. In some cases, SIEM and SOAR are deployed to satisfy compliance requirements, and from that perspective a MSSP can provide compliance reporting.

A second characteristic is the coverage of the tools serving as telemetry or log sources that are provided by the MDR service provider. The monitoring and management service is limited to the tools provided by the MDR service provider. The tools could be deployed at the perimeter, network, endpoint, a combination, or all. MSSP' coverage differ in that they monitor multiple telemetry and log sources.

The third characteristic is that the MDR service usually involves humans, but some automation may be implemented. Analysis and triage are done by analysts, and this provide for high fidelity alerts. Clients typically interact with analysts rather than looking at dashboards and other tools.

A fourth characteristic is that incident validation and remote response is provided by the MDR service provider. This means that analysis, sandboxing and reverse engineering of malware is handled by the MDR service provider. Some MDR service providers provide remediation advice. The major difference between the MSSP monitoring service and the MSSP MDR service is that with the MSSP monitoring service, the MSSP monitors the clients existing tools and critical assets as telemetry or log sources, while with the MDR service, the MSSP will install and use their own tools as log sources.

MDR service can, and are often offered from MSSP SOCs (J. Godgart, 2019)(M.K. Hamilton, 2020)(Secuvant, 2019). It is our experience that in some cases, MSSPs evolve to offer the MDR service where the MSSP provide the tools as opposed to relying on the tools provided by the client. Some examples of tools needed for a MDR

service are Intrusion Prevention Systems (IPS) and endpoint detection and response (EDR) tools. Differences between MSSP monitoring and MDR services characteristics (Zhang, 2018) are shown in Table 2.

Table 2: Difference in characteristics between MSSPs and MDR

	MSSP	MDR
Characteristic 1: Compliance Reporting	Provided	Usually not provided
Characteristic 2: Coverage	Work with multiple logs and contexts. Customer decides what logs from which telemetry sources to send	Ingests and monitors logs from own deployed security controls
Characteristic 3: Human Interaction	Normally portals and e-mail	Interact with analysts
Characteristic 4: Incident Response	Onsite and remote – need separate retainer	Onsite and remote – retainer normally included

6.3 Response service

Together with the monitoring and detection service, the incident response service is of paramount importance and a foundational service. The service work in tandem with the monitor and detect service. Events are monitored and possible malicious activity is detected. Deeper investigation is done, and eventually a single event, a couple of events or correlated events are classified as an incident. An incident could be a hots or hosts infected with malware, an ongoing attack, or data leakage.

The purpose of the incident response service is fourfold:

- Triage and investigate incidents - during this sub-task, additional research is done about the incident so that the incident can be:
- *Prioritise incidents.*
- *Severity of incident.*
- *Classify incidents.*
- *Determine impact of incident on client's environment.*
- Escalate incidents to clients.
- Response to incidents - Advise clients on how to handle the incident – this part of the service overlaps with the "Remediation Service" and includes containment, eradication, and recovery. Incident response can be automated using a SOAR.
- In the case of MDR service, orchestrate and automated response, or where the client selected a retainer from the MSSP, the MSSP engineers could provide the response on-site or remotely.

The response service should be defined, and performance metrics coupled to it. Different priorities and different severities normally have different response times associated with them. The escalation time should be agreed with the client and described in the SLA with the client. Incident response also includes remediation and containment. Remediation and containment can be performed by internal resources, co-sourced, or outsourced, and KPIs and metrics should be developed for the remediation service as well.

For guidelines on how to respond to cybersecurity incidents, consider the National Institute of Standards and Technology's (NIST) recommendations in its Computer Security Incident Handling Guide (Cichonski *et al.*, 2012). It is also a good idea to map attacks to the cyber kill chain. This shows value in that the better the SOC gets, the earlier in the kill chain attacks are detected and acted on. Consider using Lockheed Martin's "Cyber Kill Chain Methodology (Cichonski *et al.*, 2012) or the Mitre "ATT&CK Framework" (*Matrix - Enterprise | MITRE ATT&CK™*, 2022) to prove value.

In terms of an actual incident handling, frameworks such as those developed by NIST (Cichonski *et al.*, 2012) and the SysAdmin, Audit, Network and Security's (SANS) (Kral, 2012) may be considered. When choosing a framework, it is important to consider that the incident handling process will have to integrate with the client's incident handling process.

The primary services to technology mapping are done in Table 3. This mapping only considers the tools to be used to facilitate and enable the primary services. It does not consider tools for secondary services and neither does it consider tools or telemetry sources such as Intrusion Prevention Systems and anti-malware systems. SOC infrastructure tools such as jump boxes, Domain Naming Service (DNS), mail, firewalls and so on must also be considered. The infrastructure tools are outside the scope of this article.

Table 3: Primary service to technology mapping

Monitor	Detect	Response
SIEM – monitor Productivity suite	SIEM/SOAR – monitor and analysis Productivity suite	Helpdesk Incident management tool Collaboration tool Recovery tool Forensic tool Productivity suite SOAR

We will now, in Section 7 propose a Systems Engineering (SE) approach to select the correct technology. Following SE approach involves tasks such as determining user requirements and translating those to functional and technical specifications.

7. Step 4: Select technologies by applying systems engineering principles

We have in Section 6 identified the primary MSSP services and their corresponding technologies. The technology component is one of the costliest elements in a MSSP. Therefor it is crucial that a technology with the correct capability and capacity is selected. In this Section we will be viewing the SIEM and SOAR tools as systems.

The Pareto principle - also known as the 80/20 rule - states that for many events approximately 80% of the effects are from 20% of the causes (Harvey and Sotardi, 2018). Applying the Pareto principle to computing it shows that 80% of organisational risk could be addressed by 20% of the technical security controls (Symantec, 2020).

The SIEM and SOAR tools are very costly, and the Pareto principle will assist organisations to spend wisely. Experience showed that the Pareto principle could be extended to the procurement of technology. When organisations buy tools blindly off the shelf, they often utilise only 20% of the tool's capabilities, ignoring the remaining 80% of capabilities. This translates to a waste of money. A SE approach is needed to ensure that only relevant tool capabilities are identified, and that the organisation gets value for money in that at least 80% of the tool's capabilities are used.

The most important system requirement is the system functional requirement, and this will eventually lead to the technical specifications to be included in the Request For Proposal (RFP). It is recommended that the SE lifecycle is followed when selecting a SIEM / SOAR tool. The Systems Engineering Body of Knowledge (*System Requirements - SEBoK*, 2016) classifies system requirements as follows as taken from (*System Requirements - SEBoK*, 2016):

Table 4: Types of system requirement as taken from (system requirements - SEBoK, 2016)

Types of System Requirements	Description
Functional Requirements	Describe qualitatively the system functions or tasks to be performed in operation.
Performance Requirements	Define quantitatively the extent, or how well, and under what conditions a function or task is to be performed (e.g. rates, velocities). These are quantitative requirements of system performance and are verifiable individually. Note that there may be more than one performance requirement associated with a single function, functional requirement, or task.
Usability Requirements	Define the quality of system use (e.g. measurable effectiveness, efficiency, and satisfaction criteria).
Interface Requirements	Define how the system is required to interact or to exchange material, energy, or information with external systems (external interface), or how system elements within the system, including human elements, interact with each other (internal interface). Interface requirements include physical connections (physical interfaces) with external systems or internal system elements supporting interactions or exchanges.

Types of System Requirements	Description
Operational Requirements	Define the operational conditions or properties that are required for the system to operate or exist. This type of requirement includes: human factors, ergonomics, availability, maintainability, reliability, and security.
Modes and/or States Requirements	Define the various operational modes of the system in use and events conducting to transitions of modes.
Adaptability Requirements	Define potential extension, growth, or scalability during the life of the system.
Physical Constraints	Define constraints on weight, volume, and dimension applicable to the system elements that compose the system.
Design Constraints	Define the limits on the options that are available to a designer of a solution by imposing immovable boundaries and limits (e.g., the system shall incorporate a legacy or provided system element, or certain data shall be maintained in an online repository).
Environmental Conditions	Define the environmental conditions to be encountered by the system in its different operational modes. This should address the natural environment (e.g. wind, rain, temperature, fauna, salt, dust, radiation, etc.), induced and/or self-induced environmental effects (e.g. motion, shock, noise, electromagnetism, thermal, etc.), and threats to societal environment (e.g. legal, political, economic, social, business, etc.).
Logistical Requirements	Define the logistical conditions needed by the continuous utilization of the system. These requirements include sustainment (provision of facilities, level support, support personnel, spare parts, training, technical documentation, etc.), packaging, handling, shipping, transportation.
Policies and Regulations	Define relevant and applicable organizational policies or regulatory requirements that could affect the operation or performance of the system (e.g. labor policies, reports to regulatory agony, health or safety criteria, etc.).
Cost and Schedule Constraints	Define, for example, the cost of a single exemplar of the system, the expected delivery date of the first exemplar, etc.
Physical Constraints	Define constraints on weight, volume, and dimension applicable to the system elements that compose the system.

8. Mapping the conceptual process model to existing frameworks, standards and best practices

Our conceptual process model can be mapped to existing standards, frameworks and best practises. In Section 2 we stated that we will place the focus on SOC services, SOC models, mapping tools and technologies to services and SE the tools or technologies. We however include Facilities and People and Processes in Table 5 to illustrate the comprehensive coverage of our conceptual process from a framework, standards and best practice perspective.

Table 5: SOC planning steps mapped to existing frameworks, standards and best practices

Conceptual Process	Standards / Framework / Best Practice
Step1: Identify SOC services	For a list of SOC services - Towards a framework for building security operation centers (P. Jacobs, 2015). ITIL for service management (ITGovernanceUSA and IT Governance USA, 2011) Service Determination Methodology described in Section 3
Step 2: Identify SOC Models	Section 5 for methodology
Step 3: Map Technology to Services	Section 6 for methodology
Step 4: SE for Technology	SEBoK (SEBoK, 2016) ISO/IEC/IEEE 15288:2015 - Systems and software engineering — System life cycle processes
Step 5: Plan Facilities	ISO/IEC 27001:2013 Annex A11 (ISO/IEC, 2009) Occupational Health and Safety Acts (South African Government, 1993) NIST SP 800-53 (NIST, 2009)
Step 6: People and Processes	NICE Framework (NIST, 2013) SFIA (SFIA Foundation, 2015) For a list of recommended processes - For a list of SOC services - Towards a framework for building security operation centers (P. Jacobs, 2015).

9. Future work

In future studies we will identify SOC secondary services to augment its primary services. We will also catalogue the services according to SOC models. From a technology perspective, we will determine the most common functional requirements for SIEM and SOAR with the intention to map them according to industry. The intention is to develop a guide that will be useful for MSSPs when selecting their SIEM / SOAR tools. We will also develop SOC facility requirements. Further we will develop a guide to assist with SOC facility planning.

10. Conclusion

In this article we have proposed a conceptual process framework to be used when planning for the building of SOCs. The first step of our framework is to identify SOC services. We identified the three primary SOC services as monitoring, detection and response to cyber threats. We have also provided a methodology to identify the SOC services.

We then introduced the different SOC models. The SOC models will influence the SOC services, which in turn influences the SOC tools. We identified three contexts from where SOCs can be viewed. These are the consumer and service provider contexts. We the identified the different SOC models applicable to each context. The SOC models – together with the SOC services - will have an influence on the SOC tools.

In Section 6 we mapped the SOC services to its complimentary tools. And in Section 7 we proposed that a systems engineering approach be followed to identify technical specifications for the SOC tools. For each of the steps in our conceptual process there are existing frameworks, standards or best practices to guide its completion of the process, and these were introduced in Section 6.

During our research we could not find any conceptual process models that could be used to guide the SOC builders thinking when planning to build SOCs. SOC Builders can now use our conceptual process model to guide their thinking when planning for the building of their MSSP SOCs. The process will not differ much where it concerns organisational SOCs, and with small adjustments our conceptual process can also be applied during the building of SOCs with operational models different to the MSSP model.

References

C. Zimmerman and Operations Center, S. (2014) *Ten Strategies of a World-Class Cybersecurity Operations Center*, *Carson Zimmerman, MITRE*. The Mitre Corporation. Available at: www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10 (Accessed: 25 November 2018).

Cichonski, P. *et al.* (2012) *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*, *NIST Special Publication 800-61*. Gaithersburg, MD. doi: 10.6028/NIST.SP.800-61r2.

Dave Young (2020) *Security Operations Center: Insource or Outsource to MSSP?* Available at: https://www.netnetweb.com/content/blog/security-operations-center-insource-or-outsource (Accessed: 13 August 2021).

Detection | Meaning of Detection by Lexico (no date). Available at: https://www.lexico.com/definition/detection (Accessed: 27 February 2020).

Digital Hands (2021) *IN-HOUSE SOC VS MSSP*. Available at: https://www.digitalhands.com/guides/in-house-soc-vs-mssp (Accessed: 13 August 2021).

Harvey, H. B. and Sotardi, S. T. (2018) 'The Pareto Principle', *Journal of the American College of Radiology*, 15(6), p. 931. doi: 10.1016/j.jacr.2018.02.026.

HPE (2018) *What is Security Monitoring? – HPE Definition Glossary | HPE™ EUROPE*. Available at: https://www.hpe.com/emea_europe/en/what-is/security-monitoring.html (Accessed: 15 March 2018).

ISO/IEC (2009) *An Introduction to ISO 27001, ISO 27002....ISO 27008*. Available at: http://www.27000.org/ (Accessed: 25 November 2018).

ITGovernanceUSA and IT Governance USA (2011) *ITIL®– IT Infrastructure Library® & IT Service Management*. Available at: http://www.itgovernanceusa.com/itil.aspx.

J. Godgart (2019) *Ditch Your MSSP: Making the Case for Managed Detection & Response*. Available at: https://blog.rapid7.com/2019/10/07/why-do-managed-detection-and-response-mdr-services-exist-in-a-world-dominated-by-mssps/ (Accessed: 20 February 2020).

J. Miller (2019) *MDR vs. SIEM vs. SOAR Acronyms Explained | BitLyft Cybersecurity*. Available at: https://www.bitlyft.com/mdr-vs-siem-vs-soar-acronyms-explained/ (Accessed: 20 February 2020).

Jacobs, P. *et al.* (2016) 'E-CMIRC – Towards a model for the integration of services between SOCs and CSIRTs', *European Conference on Information Warfare and Security, ECCWS*, 2016-Janua, p. 350. Available at: https://books.google.co.za/books?id=ijaeDAAAQBAJ&pg=PA350&lpg=PA350&dq=E-CMIRC+–

+Towards+a+model+for+the+integration+of+services+between+SOCs+and+CSIRTs+jacobs&source=bl&ots=50kTs5LXP_&sig=vQetp1xRqVtCPukMqSi1yZgpKFU&hl=en&sa=X&redir_esc=y#v=onepa (Accessed: 19 August 2016).

Kral, P. (2012) *SANS Institute: Reading Room - Incident Handling*. Available at: https://www.sans.org/reading-room/whitepapers/incident/paper/33901 (Accessed: 26 February 2020).

Logsign (2018) *What Makes SOC Effective? People, Process, and Technology*. Available at: https://www.logsign.com/blog/what-makes-soc-effective-people-process-and-technology/ (Accessed: 4 August 2021).

M.K. Hamilton (2020) *SOC-As-A-Service & How We Differentiate | Secuvant*. Available at: https://secuvant.com/soc-as-a-service/ (Accessed: 20 February 2020).

Matrix - Enterprise | MITRE ATT&CK™ (2022). Available at: https://attack.mitre.org/matrices/enterprise/ (Accessed: 26 February 2020).

McAfee (2021) *What Is a Security Operations Center (SOC)?* Available at: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html (Accessed: 4 August 2021).

NIST (2009) *Recommended Security Controls for Federal Information Systems and Organizations*. Available at: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

NIST (2013) 'National Cybersecurity Workforce Framework', p. 127. Available at: http://csrc.nist.gov/nice/framework/ (Accessed: 17 February 2016).

P. Jacobs (2015) *Towards a framework for building security operation centers*. Available at: http://contentpro.seals.ac.za/iii/cpro/DigitalItemViewPage.external?lang=eng&sp=1017932&sp=T&suite=def (Accessed: 25 November 2018).

Robinson; Arbez; Birta; Tolk; Wagner (2015) 'CONCEPTUAL MODELING: DEFINITION, PURPOSE AND BENEFITS', in *Proceedings of the 2015 Winter Simulation Conference*. doi: 978-1-4673-9743-8/15/$31.00.

SANS Institute (2021) *Guide to Security Operations*.

SEBoK (2016) *Capability Engineering*. Available at: http://sebokwiki.org/wiki/Capability_Engineering (Accessed: 7 October 2016).

Secuvant (2019) *MDR vs. MSSP vs. SIEM – InfoSec Acronyms Explained | CI Security*. Available at: https://ci.security/resources/news/article/mdr-vs-mssp-vs-siem-infosec-acronyms-explained (Accessed: 20 February 2020).

SFIA Foundation (2015) *Why SFIA*. Available at: http://www.sfia-online.org/en (Accessed: 1 July 2016).

SOC-as-a-Service, MDR, and Managed SIEM. What's the Difference? - MSSP Alert (no date). Available at: https://www.msspalert.com/cybersecurity-guests/socaas-mdr-siem-defined/ (Accessed: 18 February 2020).

South African Government (1993) *Occupational Health and Safety Act (No. 85 of 1993)*. Available at: http://www.labour.gov.za/DOL/legislation/acts/occupational-health-and-safety/read-online/amended-occupational-health-and-safety-act/ (Accessed: 22 October 2017).

Symantec (2020) *Symantec Security Response - 80-20 Rule of Information Security*. Available at: https://www.symantec.com/avcenter/security/Content/security.articles/fundamentals.of.info.security.html (Accessed: 26 February 2020).

System Requirements - SEBoK (2016). Available at: https://www.sebokwiki.org/wiki/System_Requirements (Accessed: 26 February 2020).

The British Standards Institution (2014) *Cyber Security*. Available at: http://www.bsigroup.com/en-GB/Cyber-Security/.

Zhang, E. (2018) *What is Managed Detection and Response? Definition, Benefits, How to Choose a Vendor, and More | Digital Guardian*. Available at: https://digitalguardian.com/blog/what-managed-detection-and-response-definition-benefits-how-choose-vendor-and-more (Accessed: 20 February 2020).