SOC Service Areas: Identification, Prioritization, and Implementation

Christopher Rodman
Software Engineering Institute,
Carnegie Mellon University
Pittsburgh, PA, USA
cirodman@cert.org

Breanna Kraus
Software Engineering Institute,
Carnegie Mellon University
Pittsburgh, PA, USA
blkraus@cert.org

Dr. Justin Novak
Software Engineering Institute,
Carnegie Mellon University
Pittsburgh, PA, USA
jnovak@cert.org

***Abstract*—Organizations come in all shapes and sizes, serve myriad purposes, and exist in different security environments. But they all have one thing in common: they need security operations. How should an organization determine which services and functions its Security Operations Center (SOC) should provide? This paper identifies five factors that influence an organization's SOC service priorities. It then describes a workflow that complements standard security frameworks to efficiently determine and prioritize the services that a SOC should perform for an organization. The services that the SOC offers should complement the organization's overall cybersecurity program and align with higher level cybersecurity assessment frameworks, such as the National Institute of Standards and Technology Cybersecurity Framework. The workflow is repeatable and can be used regularly to evaluate whether SOC services continue to align with an organization's priorities in a changing world. This work will interest those responsible for the design, coordination, and implementation of security operations teams in organizations of any size.**

I. Introduction

Since the implementation of formal cybersecurity teams, cybersecurity experts have debated which functions and services those teams should offer. Those services dictate the strategy and operational models that security teams will utilize. Publications such as the Security Operations Center Capability Maturity Model (SOC-CMM) [1] identify a select number of service areas that security teams can improve upon. Additional frameworks such as the Computer Security Incident Response Team (CSIRT) Services Framework [2] demonstrate the various duties that national-level CSIRT teams can take on; however, these do not exactly align with the services that an organization's SOC will implement. Furthermore, operational models within organizational SOCs may change over time to involve services from external third parties, whereas third-party services are unlikely to influence the operations of a national-level CSIRT. Therefore, organizations should not only evaluate SOC service offerings during the implementation of the SOC but also periodically throughout the lifecycle of the SOC. Evidence of the need to shift priorities of the SOC over time is clear in annual publications such as the 2023 Data Breach Investigations Report produced by Verizon [3] and the SANS 2023 SOC Survey [4], which show different threat actor actions and how they change from year to year. The constant change in threat actions requires constant evaluation and alteration of service priorities for any cybersecurity team.

II. Purpose

When implementors determine the services for a security team, many times the answer is "It depends," a phrase that can sow uncertainty within the leadership of any organization. Other challenges manifest when organizations choose to implement SOC teams in haste during cybersecurity breaches or simply outsource SOC responsibility to third-party managed security service providers [5]. In either example, lack of preparation, planning, or direction can create ambiguity in the tactical direction of the SOC and the organizational cybersecurity program. To thwart these challenges, strategic planning of SOC services will set the foundation for determining the people, process, and technology that comprise SOC tactical operations , as described by Torres [6].

The purpose of this paper is twofold. The first is to identify existing and potential SOC services to be implemented and the factors that influence SOC service priority for an organization. The second is to formalize a workflow to complement standard frameworks to efficiently determine and prioritize the services that a SOC should provide to the organization. Such a workflow is repeatable and can be utilized on regular basis to evaluate the services that the SOC provides. Finally, the services that the SOC offer should complement the overall cybersecurity program of the organization and align with higher level cybersecurity assessment frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [7]. The paper applies directly to those responsible for designing, coordinating, and implementing security operations teams in organizations of any size.

Workshop on SOC Operations and Construction (WOSOC) 2024
1 March 2024, San Diego, CA, USA
ISBN 979-8-9894372-3-8
https://dx.doi.org/10.14722/wosoc.2024.23001
www.ndss-symposium.org

III. Defining Services of Security Teams

In his book Designing and Building a Security Operations Center, Nathans [5] identifies generalized functions of the SOC as monitoring for digital threats against an organization, conducting threat analysis, determining the risk to the organization, and conducting initial remediating actions. With the objective of identifying a standard list of functions, other publications get more specific. For example, the SOC Critical Function Guide [8] specifically identifies core responsibilities for the SOC to manage security solutions and investigate suspicious events. It breaks these core responsibilities down even further to describe phases of investigation such as alert triage, impact analysis, incident prioritization, containment, and communication. It provides guidance for implementers when building a SOC and identifies services areas of proactive detection, incident management, awareness of all IT assets, vulnerability management, and log management. In a more structured framework, SOC-CMM identifies services as security monitoring and incident management and further delineates other areas such as threat hunting and vulnerability management [9]. SOC-CMM also describes service areas from the context of building maturity of SOC teams in parallel with people, process, and technology, thereby aligning service areas with SOC maturity level. For breadth of comparison, the CSIRT Services Framework identifies an extensive list of services that national-level CSIRTs provide to their constituencies [2]. Unlike a maturity model, this framework breaks these services out into service areas, services, functions, and subfunctions.

Because there are differences in nomenclature of service areas, this study compared each guide and framework at the service level to accurately determine duties associated with each service. We then mapped the service areas across guides based on the specific responsibilities that are described in each framework. The result is a distinct map between the literature showing comparisons of service areas. I shows the high-level service areas of a SOC and CSIRT. The columns in the table attempt to align SOC service areas with the well-known publications.

Comparative analysis between the different frameworks to find a common set of service areas reveals the gaps between the frameworks. While each framework serves dissimilar purposes, they can aide in the identification of a standard set of service areas that can be used when designing a SOC. High-level service-area activities such as Threat Intelligence and Threat Hunting can be collapsed into Situational Awareness because their activities produce artifacts for attack indicators and activities to proactively discover attack paths in an environment. The same can be done for Security Monitoring and Log Management with alignment to Information Security Event Management. This leaves the following services areas that encompass functionality between the three guides and frameworks: Security Monitoring, Security Analysis, Information Security Incident Management, Information Security Event Management, and Knowledge Transfer.

TABLE I
High-Level Service Areas of SOCs and CSIRTs

SOC CMM	**(CREST) SOC Critical Function Guide**	**CSIRT Services Framework**
Security Monitoring	Proactive Detection	
Incident Management	Incident Management	Information Security Incident Management
Threat Hunting		Situational Awareness
	Awareness of All IT Assets	Situational Awareness
Threat Intelligence		Knowledge Transfer
Vulnerability Management	Vulnerability Management	Vulnerability Management
Security Analysis		
Log Management	Log Management	Information Security Event Management

Furthermore, these proposed service areas can easily be mapped to cybersecurity program frameworks such as the NIST CSF [7] to provide alignment with the control functions implemented within an overall security program. IITable II demonstrates the alignment of our proposed SOC service areas with the five functions of the NIST CSF.

TABLE II
SOC Service Areas Mapped to NIST CSF Functions

NIST CSF Function	**SOC Service Area**
Identify	Situational Awareness
Protect	Security Analysis
Detect	Security Monitoring, Information Security Event Management
Respond	Information Security Incident Management
Recover	Knowledge Transfer

While a SOC can perform either some or all of these service areas, it is important to use specific motivating factors when prioritizing the service areas that the SOC will operate in.

IV. Factors that Influence Services a SOC will Prioritize

If you knew you were going to be the victim of a cyber-attack, would you conduct security measures within your organization differently? Factors, both internal and external, to an organization will ultimately influence what services a developing SOC will prioritize. Research by M. A. Majid and K. A. Z. Ariffin identified people, processes, and technology as critical factors and managerial support, financial, and continuous improvement as secondary factors that affect the development and implementation lifecycle of a SOC [16]. Diving deeper, we identified legal and regulatory requirements, organizational culture and risk acceptance, budget, security risk assessment outcomes, and existing security controls and infrastructure as major factors that will influence the services a developing SOC will prioritize. Each of the factors we identified, with the exception of legal and regulatory requirements, tie back to one or multiple of the critical or secondary factors outlined by Majid and Ariffin. One factor not mentioned in their research are legal regulatory requirements, which will subsequently influence each of the factors identified. This list is not inclusive to all potential factors, but those most common and critical.

A. Legal and Regulatory Requirements

Security and privacy regulations have been implemented across the globe since the United States enacted the Privacy Act of 1974, protecting personally identifiable information. Widely accepted examples today include the General Data Protection Regulation (GDPR) in the European Union and the Sarbanes–Oxley Act, Payment Card Industry Data Security Standard (PCI DSS), and Health Insurance Portability and Accountability Act (HIPAA) in the United States. Specifically, within the United States, a SOC within a financial institution must comply with PCI DSS, while a health care organization must comply with HIPAA. These requirements may drastically affect how a SOC prioritizes which services to provide.

What part of the world a SOC or, more specifically, its data resides in will determine the legal and regulatory requirements that a SOC must adhere to. If a SOC is physically located in the United States but uses a cloud provider that backs up its data in Brazil and Denmark, it will be required to adhere to the applicable legal and regulatory requirements of not only the United States but also of Brazil and Denmark. Sound complicated yet? Luckily for cloud service customers, cloud service providers (CSPs) take on a significant amount of that responsibility with the Shared Responsibility Model [10]. This means that security of the cloud (e.g., infrastructure, physical security, application security) is the responsibility of the CSP. Security in the cloud (e.g., security of users, endpoints, network, data) is the responsibility of the customer. Let's take it one step further. Even if an organization is positioned strictly within the borders of the United States, if it possesses data of non-U.S. citizens, such as data from citizens of the European Union, then that organization will be required to adhere to additional legal and regulatory requirements, such as GDPR.

Whether internal or external to an organization, the type and location of the data that a SOC manages will determine what legal and regulatory requirements it must comply with, thus determining what security controls and services the SOC must have in place.

B. Organizational Culture and Risk Acceptance

Culture is the set of beliefs, values, attitudes, systems, and structures that make up an organization and in comparison to other quantitative factors, is more volatile and specific to the operational nature of the organization. This culture is influenced by many factors: business goals and objectives, regulatory requirements (as previously mentioned), financing and budgetary restrictions, and stakeholder interest, to name a few. Further studies by D'Arcy and Havov [13] identify impact and effectiveness of organizational cybersecurity awareness training programs based on factors such as employee demographics, working modality and technical proficiency. This research demonstrates the impact of organizational composition and operating models to effectiveness of cybersecurity awareness programs. Because culture has such a momentous impact, it directly affects the people, processes, and technology of that organization. It is important to understand that culture is based on behavior over time. Studies conducted by Herath et. al [14] demonstrate reduced levels of moral disengagement in accordance with cybersecurity policies is reduced by simply agreeing on and communicating information security policies. In our context, increased engagement with security policies can lead to positive security culture within an organization. Further studies elaborate on the need for security awareness training, specifically pointing out the existence of awareness policies and programs, but also considering the audience and their pre-existing awareness and knowledge levels [15]. From these studies we can infer organizational security culture based on the existence of security awareness within the organization.

How does culture affect risk acceptance? Based on the previous section the presence of cybersecurity awareness programs or at minimum their policies is a reflection of overall cybersecurity culture of the organization. Therefore, an organization without sound security culture, could unknowingly accept unintended risk [15]. Simply put, what is an accepted risk for one organization may not be accepted at another. For example, many financial institutions have a certain level of accepted risk because many have legacy systems within their environment. These systems are machines that are no longer being supported by the manufacturer (e.g., mainframes). For many, the risk of replacing these machines is not worth the potential business disruption or loss of company data.

As it relates to risk acceptance, culture has a direct impact on an organization's Risk Management program (which includes risk acceptance guidelines). This subsequently affects which services an organization will prioritize for its SOC. It might sound backward that organizations will accept certain risks, but according to Snedaker and Rima, "the most common reason is that the cost of other risk management options, such as avoidance or limitation, may outweigh the cost of the risk itself. There is no benefit in spending $100,000 to avoid a $10,000 risk" [11]. But again, an organization's culture and regulatory context determine the risk it accepts.

C. Budget

The best time to ask for a security budget is right after a breach. Of course, as security professionals, managers, C-level executives, and other stakeholders, we want to prevent an incident from occurring in the first place. However, we need to understand that a security breach is not an if but a when. The amount of financial backing a SOC has will be one of the biggest factors determining the prioritization of services a SOC will provide. With a limited security budget, the "nice-to-haves" will fall further down the list to make room for the "must-have" functions. Legal and regulatory requirements must be prioritized before additional security measures can be implemented. According to Quilter, “A good security budget encompasses security programs’ tactical and long-term strategy needs and maps clearly and transparently to the business’ operating plans” [12]. The services a SOC provides should directly align with the organization’s mission, goals, and overall cybersecurity program. Risk assessments are further discussed in the next section, but it should be noted here that both security planning and budgeting processes should be informed by an annual security risk assessment. Whether a risk assessment maps directly to the NIST CSF or another framework, a SOC cannot adequately budget and prioritize SOC services without first knowing what risks are present within the organization. Additionally, while there are many open-source resources and tools available that a SOC with a limited budget may use, it is more than likely that only sufficient support and financial backing will address many of the larger security risks or gaps identified by an annual security risk assessment, which will ultimately affect how or which services that SOC will prioritize moving forward.

D. Security Risk Assessment Outcomes

Whether a security risk assessment is performed as part of an internal policy, regulatory requirement, or voluntarily, the outcome inevitably affects how an organization will prioritize SOC services. A security risk assessment, such as one mapped to the functions and categories of the NIST CSF [7], will help identify the current security controls in place and where security gaps are present, within the scope of the assessment. The identified risks are then assigned ratings based on likelihood and criticality. Building from Section III, an assessment of an organization’s security controls according to the NIST CSF, can directly influence the services that either currently exist or are to be desired by the SOC. Linking the priority levels of the NIST CSF to prioritize SOC services requires an organizational risk assessment based on the controls present by the outcome of NIST CSF discovery. Security controls that address organizational risks with a high likelihood and a high criticality rating will be of greater importance to remediate than a risk with a low likelihood, even if that risk would be highly critical.

A security risk assessment informs an organization about the threat landscape of the people, processes, and technology associated with it, within the confines of the assessment scope. As part of those ratings assigned to the risks identified during the assessment, a prioritized outline will be presented to the security team, which could subsequently serve as a guideline to assist the SOC in prioritizing the services provided. It would not make sense for a SOC to prioritize a service if it would not assist in remediating risks.

E. Existing Security Controls and Infrastructure

No matter how long an organization has been established, there are more than likely already some security controls in place to protect organizational assets and infrastructure. Whether managed internally or by a third party or cloud provider, these pre-existing controls will help shape what services a developing SOC will prioritize. It probably goes without saying that an organization established 30 years ago will probably have more robust security controls in place and be more mature, overall, than an organization that has been around for only 5 years. This already-laid foundation will serve as the groundwork for a developing SOC and will dictate which SOC services the organization needs and how to prioritize them.

F. The Bottom Line

Even if your organization has the largest security budget in the world, that does not mean a developing SOC should implement all possible SOC services at one time, or even ever, for that matter. Each SOC is unique, and the way SOCs serve their organizations is not one-size-fits-all. Developing a functioning SOC takes time, resources, and qualified individuals. There is no one right way to serve your constituents or your organization. When planning and prioritizing which services your SOC will provide, consider legal and regulatory requirements, organizational culture and risk tolerance, budget, and existing security controls and infrastructure. From these influential factors, you can begin to determine what attributes to consider when assessing SOC teams and use them to inform a repeatable process to run at regular intervals.

V. Implementing SOC Functionality

The preceding discussion outlines a process to identify SOC functions, based on established frameworks, and then prioritize them based on organizational needs. However, to complete the process of implementing SOC functions, organizations must still have a process for matching SOC functions to business needs. By doing so, an organization can implement a SOC that has the capabilities needed to support organizational goals, while reducing or eliminating entirely any superfluous functions that act only as cost centers without providing sufficient return on investment. In practice, this is where organizations must make the leap from general security goals and risk assessments to identifying SOC solutions that address those challenges.

We present here a formal SOC function-prioritization workflow which outlines how organizations may go about this process, ultimately resulting in the maximization of SOC responsiveness to organizational needs. This five-phase workflow, shown in Figure 1, may be used to develop an initial SOC capability or to implement additional capabilities in an existing SOC.

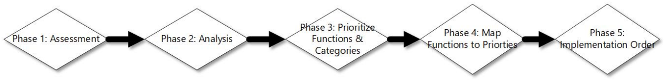
Phase 1: Assessment
Phase 2: Analysis
Phase 3: Prioritize Functions & Categories
Phase 4: Map Functions to Priorties
Phase 5: Implementation Order

Fig. 1. Workflow for prioritizing SOC functions

Section IV identified and described factors that influence how a SOC may determine which services to prioritize or which functions it may perform. While understanding risk may be the most important of these factors, there are many others an organization must explore and understand.

A. Implementation Phases

The process of identifying and describing factors that influence SOC services is part of the first phase in the SOC function-prioritization workflow, which is to conduct an assessment of the SOC, its parent organization, and any related functions. The overall objective of this workflow phase is to determine organizational security objectives and to describe the current as-is state of security operations within the organization and any existing SOC capability. Once this assessment is complete, the organization should have the data and information it needs to proceed with developing new capabilities. This data and information should include things like an asset summary or critical asset inventory, a data summary including types and classifications of organizational data, and a description of a desired to-be state of the security for the listed assets and data.

As it relates to the identification of factors such as risk, as noted above, those factors should largely serve to determine the to-be state for SOC function and overall organizational security. For example, an organization may determine that data sensitivity is a significant concern, and therefore is a factor that will influence SOC services. If such an organization is not comfortable opening its systems to external audits or post-incident analysis, then it will have to execute functions such as penetration testing or malware analysis internally. Therefore, these services must be part of any described to-be SOC end state.

Once the initial assessment is complete, the organization analyzes the data and information in Phase 2. This analysis will largely focus on bridging the gap between the as-is and the to-be states. Once these states are defined, the organization should conduct a gap analysis. It is important to note that through this phase, the organization should define and discuss any issues or challenges in terms of SOC functions. For example, if the organization identifies that the as-is state includes a robust security information and event management solution, it may say that a log collection and analysis function or service exists. In this way, the organization can view the outcomes of the gap analysis not as a list of problems to solve but rather as a list of SOC functions to add, as shown in Figure 2.

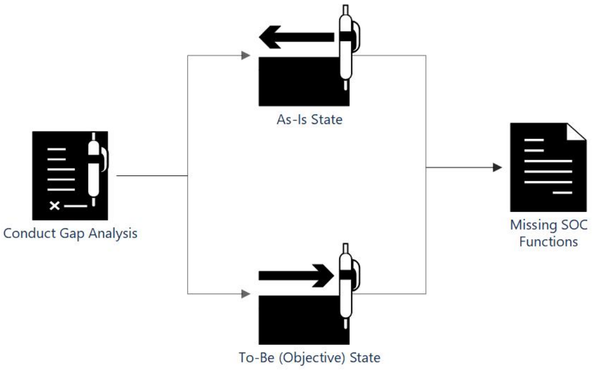

Fig. 2. Outcomes of gap analysis

Phase 3 of the workflow, prioritize NIST CSF functions and categories, may be done in conjunction with Phase 2 or immediately thereafter. Phase 2 is the correct place for an organization to completely understand its specific organizational needs, while Phase 3 is the opportunity for organizations to consider those needs in a larger context, such as that of the guidance provided by the NIST CSF. This process of consideration should build upon a larger understanding of any factors that influence the organization's priorities. For example, Section IV above notes several of these potential factors, including regulatory requirements, risk culture, and budget. If, for example, an organization needs to be GDPR compliant, implementing NIST CSF functions and categories that ensure compliance must be prioritized over other functions, regardless of other factors, including cost.

Once the list of missing SOC functions (Phase 2) and the prioritization of NIST CSF categories (Phase 3) is complete, organizations may move on to Phase 4, mapping those functions to corresponding priorities. In this phase, organizations pivot from general security goals and risk assessment to identifying SOC solutions that address them, which is the core purpose of developing a new SOC or SOC capability. The mapping should reach back to motivating factors and influences identified by the organization. Continuing the example above, if the motivating factor for an organization was the presence of GDPR regulations, and those regulations led an organization to identify the Data Security (PR.DS) Category under the Protect function of NIST CSF as a priority, then the organization must be able to protect data at rest, in transit, or in use. For a SOC to support this mission, that SOC must be able to perform audits of the data and its protection mechanisms. Therefore, Audit and Assessment is a function or service that the SOC should offer.

In Phase 5, the final phase of this workflow, organizations must begin thinking about implementation. This workflow does not address implementation directly; rather it suggests that the final step for developing a list of SOC functions or services should be to identify the order in which those new functions should be developed and implemented within an organization. To do this, organizations must consider the people, processes, and technologies (PPT) required to make those functions successful within their operational contexts. PPT are considered the core pillars of SOC functionality [6], the three elements that an organization must develop to have a capable function. To implement a new capability, an organization therefore must understand what people must be hired or trained, what equipment must be procured, and what policies must be put in place. The organization must then evaluate the resources required to do all the above. This exercise, along with an understanding of the influencing factors discussed in Section 2, will help decision makers choose which new SOC functions they should implement first.

Future Work: Beyond the determination of specific service areas and their priorities, SOC teams and their leadership could benefit greatly from regular evaluation of the SOC people, process and technology attributes contained within each service area. Such a framework of reference could be a valuable tool when applied in regular assessment intervals as described by this study. This would provide SOC implementors with exact instruction for components required to build a successful, organizationally tailored SOC even when organization priorities change.

VI. Conclusion

In conclusion, this study explored the impact of uncertainty when establishing the responsibilities of the SOC and identified service areas that will influence the remaining maturity phases across several different models. These service areas—Security Monitoring, Security Analysis, Information Security Incident Management, Information Security Event Management, and Knowledge Transfer—can be influenced by several different factors during design and implementation. These factors encompass organizational culture, budget, existing architecture, and emerging technologies, to name a few. Finally, this study described a repeatable process that organizations can use to determine the most appropriate service areas to implement as part of assessing a SOC, building maturity, and aligning with organizational cybersecurity objectives.

Acknowledgment

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

DM24-0016

References

[1] R. Van Os, *SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers.* National Library of Sweden, 2016. https://urn.kb.se/resolve?urn=urn:nbn:se:ltu:diva-59591

[2] *CSIRT Services Framework Version 2.1. FIRST—Forum of Incident Response and Security Teams*, n.d. Retrieved November 27, 2023. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

[3] *Data Breach Investigations Report.* Verizon, 2023. https://www.verizon.com/business/resources/reports/dbir

[4] C. Crowley, J. Pescatore, and B. Filkins, *SANS 2023 SOC Survey.* SANS Institute, 2023. https://www.sans.org/white-papers/2023-sans-soc-survey/

[5] D. Nathans, *Designing and Building a Security Operations Center.* Elsevier, Syngress: 2015.

[6] A. Torres, *Building a World Class Security Operations Center: A Roadmap* (p. 12) [White Paper]. SANS Institute, 2015.

[7] *Cybersecurity Framework.* NIST, 2013. https://www.nist.gov/cyberframework

[8] *SOC Critical Function Guide.* CREST, 2018. https://www.crest-approved.org/wp-content/uploads/2022/12/SOC-Critical-Function-Guide.pdf

[9] R. van Os,*SOC-CMM: Measuring Capability Maturity in Security Operations Centers.* SOC CMM, n.d. Retrieved March 15, 2023, from https://www.soc-cmm.com/

[10] *Shared Responsibility Model - Amazon Web Services (AWS).* Amazon Web Services, Inc., n.d. Retrieved January 9, 2024, from https://aws.amazon.com/compliance/shared-responsibility-model/

[11] S. Snedaker and C. Rima, *Risk Mitigation Strategy Development. In Business Continuity and Disaster Recovery Planning for IT Professionals* (pp. 337–367). Elsevier, 2014. https://doi.org/10.1016/B978-0-12-410526-3.00006-4

[12] J. D. Quilter, *Dealing with Security Budget Challenges.* Security Executive Council, 2018. https://securityexecutivecouncil.com/insight/security-program-strategy-operations/dealing-with-security-budget-challenges-1308

[13] J. D'Arcy and A Hovav, *Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures*, 2008

[14] T. Herath et al, *Examining employee security violations: moral disengagement and its environmental influences*, 2017

[15] T. Lejaka, A. Veiga and M. Loock, *Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa*, 2019

[16] M. A. Majid and K. A. Z. Ariffin, *Model for successful development and implementation of Cyber Security Operations Centre (SOC)*, 2021