EDPACS

The EDP Audit, Control, and Security Newsletter

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/uedp20

A MATURITY CAPABILITY FRAMEWORK FOR SECURITY OPERATION CENTER

Issam Taqafi, Yassine Maleh & Karim Ouazzane

To cite this article: Issam Taqafi, Yassine Maleh & Karim Ouazzane (2023) A MATURITY CAPABILITY FRAMEWORK FOR SECURITY OPERATION CENTER, EDPACS, 67:3, 21-38, DOI: 10.1080/07366981.2023.2159047

To link to this article: https://doi.org/10.1080/07366981.2023.2159047

Published online: 29 Dec 2022.

EDPACS
THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

2023 VOL. 67, NO. 3

A MATURITY CAPABILITY FRAMEWORK FOR SECURITY OPERATION CENTER

ISSAM TAQAFI, YASSINE MALEH AND KARIM OUAZZANE

Abstract. Owning a Security Operation Center (SOC) is becoming increasingly common for organizations as part of their cybersecurity strategy to ensure near-real-time detection and adequately respond to cyber-attack engaging the SOC's humans, technology, and processes. However, SOC investments only sometimes achieve the best possible outcomes and only provide an acceptable protection level in some cases due to the challenges related to the technologies, processes and especially the human factor. This paper proposes a new practical maturity framework for Security Operation Center. This will serve as a roadmap for IT auditors and security experts when they evaluate the maturity of a security operation center in terms of safeguarding the assets of the company, its partners, and its clients.

INTRODUCTION

Security operations centers should be analyzed as a management tool for the continuity and quality of the organizations' operations. Their inclusion in their organizational structure will allow organizations to achieve their strategic objectives. It should be borne in mind that the dissemination of the use of Information and Communication Technologies (ICT) has changed our daily activities and how we interact with each other as individuals and with companies, organizations and governmental entities, organizations and governmental entities.

This increased use of systems, technologies, and communications leads to an increase in cyber threats that take advantage of vulnerabilities to obtain economic benefit through the theft of money, money laundering, and financial benefit through the theft of money or intellectual benefit through patent infringement. patents. This problem has led to the emergence of the computer science field, the area of the study of computer security, whose objective is to guarantee the integrity, confidentiality, and

availability of the data and availability of data and processing systems (Miloslavskaya, 2018).

Computer security requires a combination of technical knowledge of all computer platforms and management knowledge to articulate devices, technologies, advanced detection systems, processes, and people. In this way, it will be possible to effectively and sustainably protect the assets of interest to the organization (Maleh, 2018).

A SOC is a team of security experts in charge of monitoring, detecting, analyzing and qualifying security events. This team ensures the management of appropriate reactions to proven security incidents. For some organizations, this team administers and controls the day-to-day management of security systems and measures; for example, the "hardening" of standard operating systems to reinforce their security, or the management of accreditations (access rights to resources) or even the management of "patch management." In direct support of the business and partnership with IT services, a SOC aims to reduce the duration and the impact of security incidents that take advantage of, disrupt, prevent, degrade or destroy systems dedicated to standard operations. This is achieved through effective monitoring and tracking of incidents from end to end. The SOC is responsible, on the one hand, for declaring that there is indeed an incident on the IS, and, on the other hand, it is responsible for conducting the operations that will enable it to declare the incident closed. From an operational point of view, it is the combination of the SOC and CERT/C-SIRT entities that ensures the resolution of an incident (Maleh, 2021).

The overall objective of the paper is to demonstrate that a security operations center (SOC) is a management solution to the problem of cyber defense. To achieve the general objective, it will be necessary to address the first specific objective, which is to introduce security operations, including the reasons behind creating a SOC and its services. Then we will move on to the second specific objective, which is to explain the triad of processes, people and technologies, whose synergy and interaction support the management of a SOC. Finally, the third specific objective will be developed to outline the strategy for creating a maturity model for SOC.

BACKGROUND

There needs to be more literature on security operations centers. Only a few studies on security operations centers have been published in the past ten years. Most of the material about security operations centers is based on presentations and blogs from security vendors and best practices. There are few studies on security operations centers (Chamkar, 2022).

The first-generation security operation centers were created in the early years of the internet. Antivirus software and firewalls were the initial security elements. Monitoring these elements and taking appropriate action in the event of potential threats or events was the responsibility of the security operation center, which was often a single person in those days. The fifth generation of security operation centers, which concentrate on processing massive data sets, has developed over time. This emphasis also covers the business environment and corporate hazards (Hewlett Packard, 2013).

The 2013 Hewlett Packard paper offers important details on the objectives of a security operation center. But it must offer guidance on how security operation centers must be set up. Security vendors like IBM (Meenan & Laurens, 2015), HP (Hoffmann, 2014), and Ernst & Young have released presentations and whitepapers on best practices for designing and implementing security operation centers, and they may be found on their respective websites.

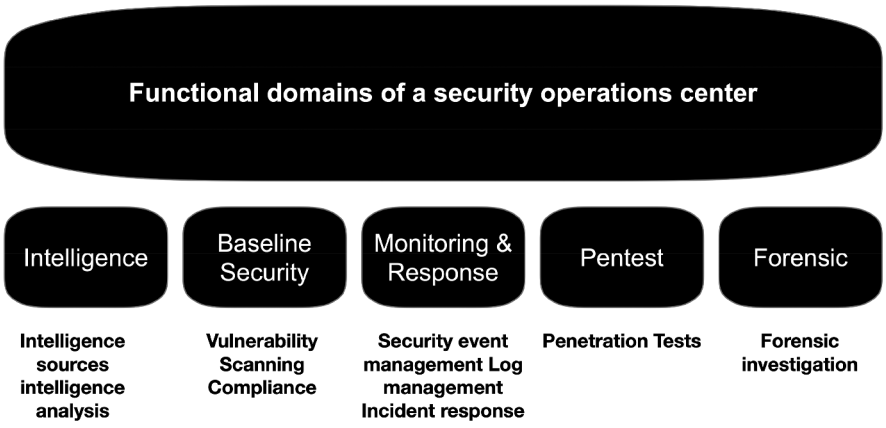
Since these media promote their products and services, the information included might be considered somewhat subjective. In his study on gauging capability maturity in security operations centers, Van Os (Van Os, 2016) comes to the same result.

There are few studies on security operations centers, and each author approaches the topic differently. A security operations center's objectives and functional domain are broadly outlined in Michail's (2015) research paper. The following paragraph goes into more depth on the functional domains indicated in the study report and is also explored by Schinagl, Schoon, & Paans (2015) and Jacobs et al. (2013). The objectives outlined in the study by Michail (2015) are, to a considerable part, identical to those discussed in the research paper by Kelley & Moritz (2006), which examines the best practices of a security operations center (2015). Hoffman (2014, p. 5) made an intriguing point on the breadth of the security operations center. A security operations center's initial emphasis was on perimeter security. With time, a security operations center's emphasis switched from protecting the company to protecting the applications.

Functional Domains of a Security Operations Center

The duties of a security operations center are grouped by domain in (Michail, 2015), Schinagl, Schoon, & Paans (2015), and Jacobs et al. (2013)'s writings. Functional domains are the names for these primary emphasis areas. The security operations center has a variety of duties and tasks, depending on how an organization is set up. Figure 1 below shows SOC functional domains.

Figure 1 ***SOC Functional domains.***



Intelligence Function

The security operations center's main task is intelligence gathering. In this field, choices are made on what to do in the face of threats or security incidents. The security information that the intelligence domain receives through internal monitoring feeds, baseline reports, or external threat reports is what it uses to operate. In this area, threat and security event analyses are carried out.

Baseline Security

To prevent security mishaps, compliance and vulnerability checks are crucial. Security awareness based on compliance and vulnerability assessments is crucial in the ICT ecosystem. Deviations are reported for the intelligence team's further attention.

Monitoring and Response

Monitoring your ICT environment can inform you how your network's traffic behaves. Anomalies may be quickly found and possible risks can be addressed early by analyzing your network's system behaviors and traffic patterns.

Organizations use Security Incident & Event Management software to gather all the traffic patterns and log data from ICT systems.

Pentest

Organizations frequently use penetration testing to identify security flaws in a specific system. To prevent security flaws in live systems, penetration testing is done as part of the development process. However, live systems are also tested when fresh dangers and weaknesses appear.

Forensic Investigation

A forensic investigation is conducted when a significant security issue necessitates a thorough investigation into the threat actor and the root cause. Forensic evidence should be appropriately protected if this information is given to local authorities. The proof these investigators provide, such as log files, scrambled hard drives, etc., aids local law enforcement.

People, Process, and Technology Perspective

Given the functional areas, a security operations center needs people, processes, and technology to achieve its objectives. This paradigm is comparable to Jan van der Berg's (2018) three-layer approach, in which the technical, social-technical, and governance levels are defined. These viewpoints are further explained in the sentences that follow.

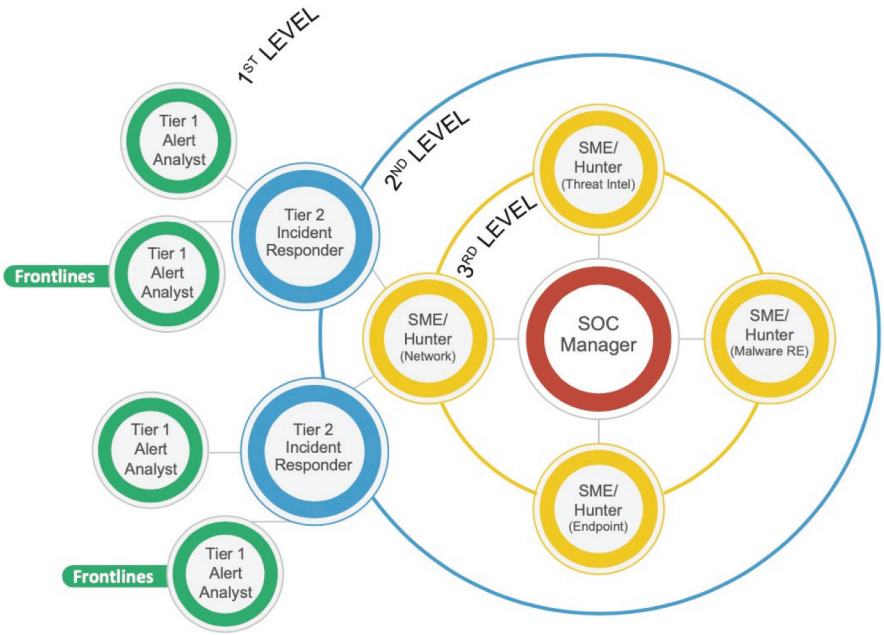
People

It is frequently asserted that in a security operations center, people matter. When responding to alerts or occurrences, humans may provide decision context. The number of staff varies depending on the duties of a security operations center. However, most security operations centers feature a manager and security analysts. The degree of knowledge varies depending on a security analyst's duties and activities (Exabeam, 2019). Figure 2 below shows Functions in a security operations center.

The level of security analysts can be classified as follows:

- Level 1 security analyst: The first level security analyst is in charge of keeping an organization's systems and infrastructure under observation. Responding to alarms, triaging alerts, and supplying the security analyst level 2 with the necessary security data for additional investigation.
- Level 2 security analyst: Based on numerous security inputs, level 2 security analysts examine situations. Relating the data and taking appropriate action to address or prevent any additional harm to the company.
- Level 3 security analyst: The subject matter expert is another name for the level 3 security analyst. This individual is an expert in a certain specialty area, like malware or threat intelligence. Its main objective is to take measures to avert incidents proactively. Additionally, a security level 2 analyst may request professional assistance from a security analyst level 3 anytime.

Figure 2 ***Functions in a security operations center.***



Process

The processes of a security operations center are discussed from various perspectives in the literature. An Escal Institute of Advanced Technologies white paper claims that, Various points of view on a security operations center's functioning may be found in the literature. The Escal Institute of Advanced Technologies published a white paper on the subject "Computer Security Incident Handling Guide" (Cichonski, Millar, Scarfone, & Grance, 2013). Many diverse perspectives on a security operations center's processes may be found in the literature, according to the findings presented in a white paper that was put forth by the Escal Institute of Advanced Technologies (Hoffmann, 2014). The processes added to those used to respond to security incidents are done at the firm's discretion and depend on the responsibilities.

Technology

A monitoring solution is at the heart of effective security operations centers. This monitoring solution can collect, detect, aggregate, and analyze log data from various systems. Examples include network appliances, firewalls, mail filters, antivirus software, intrusion detection systems, intrusion prevention systems, proxy services, and business applications. A Security Information & Event Management system is the monitoring system utilized by most security operations centers.

Security Operations Center Challenges

Constant pressure is put on security operations centers to ensure their enterprises' safety and forestall any security breaches that may occur. Given that every vulnerability within a company might result in security breaches, this is an extremely difficult undertaking. The main challenges (Crowley & Pescatore, 20198) that security operations centers face nowadays are:

- Managing the growing amount of security alerts. The volume of (log) information that requires analysis, triage, and follow-up inside an organization grows continually as new systems and devices are added. Is it possible for security analysts to keep up with the increasing quantity of security warnings, and, more importantly, are they focused on genuine security alerts and threats?
- Technology is different. As part of the functional domains, security operations centers have vast responsibilities. Each of these disciplines has its own set of systems and tools. These systems and tools serve to automate jobs and increase productivity; nevertheless, they also need the security operations center to maintain, train for, and work with a variety of systems and tooling.
- People. There is a skilled labor shortage in the security business. There is a greater demand for educated persons

than is available. It is also more difficult to obtain education in the security arena. Years of education, training, and experience are required.
- Budgets. How much money is a company ready to spend on security? There is no such thing as 100% security. As a result, the question remains as to how much risk the company is willing to assume. What is the risk level?

A security operations center's difficulties are closely related to the people, process, and technology perspectives discussed in the preceding sub-chapter.

METHODOLOGY

Based on the research design methodologies, this study will use a pragmatic paradigm (McKenney & Reeves, 2013). The data will be mostly qualitative, and the research will be conducted using inductive logic. Academic literature, reference books, and numerous referential and best practices, such as NIST, ISACA, OWASP, and ISO 27,000, are used to collect data.

This study will rely heavily on qualitative data and use inductive reasoning to conclude. The collected information is based on numerous best practices and reference standards from organizations like NIST, ISACA, OWASP, and ISO 27,000 as well as scholarly articles and publications (Johnson, 2014).

This study will be conducted as a qualitative descriptive study, with data obtained from a community sample but validated by subject matter experts in cybersecurity. Second, this investigation's solution phase will make use of design science. Research in the field of design must culminate in a practical outcome, such as a construct, model, technique, or instantiation (Hevner & Chatterjee, 2010, p. 9). It is possible that a remedy to the identified root-causes already exists based on existing best practices; otherwise, a new 'artifact' will be produced.

Different observational methods are used to collect the available data. The following data collection methods are used (Edgar & Manz, 2017):

- Examination of the relevant literature: In the context of the review of relevant literature, numerous existing case studies and reference material connected to cyber security will be explored to form the theoretical foundation for SOC.
- Interviews that are only partially structured will be conducted with a large number of cybersecurity professionals to obtain in-depth qualitative information on the present status of SOC components.

Understanding how, when, and why a theory works or doesn't function is essential to elucidate the linkages between theory and practice. This technique plays a crucial role in this endeavor.

THEORETICAL FRAMEWORK

The road to the current existence of standards and laws has been forced, as standards emerged reactively in the face of undesired events rather than proactively. Similarly, the everyday

responsibilities of a security operations center are the result of years of evolution and reorganization in the responsibilities of the areas that make up a department in charge of systems and telecommunications.

Over time, specific areas have been created to manage IT security, whose responsibilities could originally be found among those of a data network or server administrator. Looking back, it is possible to identify different generations or levels of maturity of security operations centers.

The first generation of what we know today as a security operations center (SOC) was a set of responsibilities scattered among areas of the systems department exercised by people whose primary task was other and who were therefore not trained or security aware. Their tasks consisted of monitoring network devices and servers to ensure the availability of services, basic administration of antivirus systems, and a limited collection of audit logs for network devices.

The combination of human resources, technology, and processes should be articulated with collaboration and communication to respond to identified needs. Finding the balance between shaping a SOC according to global practices while delivering the services immediately needed by the organization will be an ongoing task for middle and senior management.

The security operations center plan must be aligned with the information systems and technology strategic plan, which in turn must be aligned with the organization's strategic plan to support the operating model determined by senior management. This alignment will ensure that human and financial resources are allocated to protect the assets that are of interest to the organization. Without this guidance, a false sense of security can be created. The security operations centers will then have their scopes, missions, operating, and development models at each stage, which will be derived from the strategic plans.

Outlining these guidelines will serve as a guide for each stage of planning and the daily operation of the analysts. Considering budget constraints and finite resources, risk management appears helpful in prioritizing and allocating resources. Outlining the strategy of a security operations center will involve knowing the cybersecurity challenges facing the organization, what the roles and responsibilities of a SOC are, what processes need to be put in place, and what technologies will support management.

The SOC infrastructure is based on temporary IT technologies, which can be pervasive. Let us focus on the most necessary set of SOC software and hardware, providing automation of its activities. Analyzing detected events, incidents, and information security vulnerabilities should be automated as the most labor-intensive and important. This is necessary to create a single point for collecting and managing all additional information. To ensure the entire lifecycle of an event, incident, or vulnerability, starting with the assignment of an analyst to be responsible for handling it and ending with the action needed to resolve it. If to follow the best practice of automation of business processes, the system of GRC class (Governance, risk management, and

compliance) integrated with other software and hardware means SOC and external systems can act as the primary means of automation of SOC activity. The functionality of GRC systems allows:

- Identify and maintain centralized accounting of assets to be protected and assess their value;
- Store and update the library of SOC administrative documents;
- Maintain a unified database of incidents and the history of their processing in an automated mode;
- Conduct training and knowledge testing of employees;
- Automate procedures for incident classification and registration, notification of responsible persons, and escalation;
- Monitor and evaluate the effectiveness of SOC activities.

In addition to the above, GRC systems automate practically any SOC process. These systems accumulate knowledge about company assets, predetermined risks, and employees. Using GRC systems, SOC employees quickly get access to information on the criticality of the incident-affected assets, information on their owners, quickly form necessary reporting and provide top management and asset owners with an opportunity to control SOC efficiency. As a budget alternative to GRC, it is possible to use the Service Desk or Help Desk systems already in place in a company. It will be necessary to modify them to meet new requirements, such as automating the processing of events from external analytical systems. Still, on the whole, such a solution will be cheap enough and have the minimum required functionality for incident management. SIEM (Security information and event management system) is the basis for the automated collection, storage and analysis, and separation of information security events from the events generated by all IT systems of the company. This system is the basis for identifying IS events and conducting operational and retrospective investigations of IS incidents. It also provides a toolkit for identifying almost any malicious activity or cause of technical failure on a company's network. Specialized scanners and configuration analysis systems are used to detect vulnerabilities in SOC. For example, they allow automation control of compliance of network equipment settings with specified corporate policies, inventory of protected assets, and identification of vulnerable software versions. The data they collect must be available immediately to SOC staff as an index to the policy.

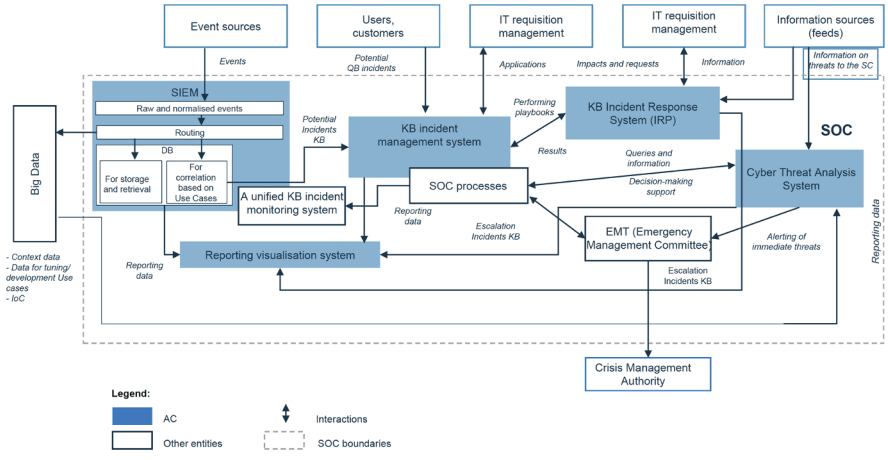
It is necessary to mention that SOC employees should be involved in SOC to function appropriately, and all employees of the protected company as well because the company's safety depends on their actions and adherence to the procedures. It is with them that protection begins, and it is thanks to their vigilance, SOC staff can detect and inform SOC employees of possible information security events and vulnerabilities.

The systems outlined are both a "must-have" set of systems that can be used to assess the possible consequences and scenarios of attacks and security breaches, and to identify and remedy their causes. The systems outlined are what we call a "must-have" set. But it can also be adjusted depending on the maturity of the company or the level of development of the response center. Additional toolkits include systems such

as - systems to prevent leaks of confidential information; - systems to investigate incidents and collect evidence; - systems to avoid denial of service attacks. Figure 3 shows the interaction scheme of the specified set of technical means and information flows.

The realities of today's information world impose additional requirements on the center's tools. The first is the so-called Big Data infrastructure. The volume of information generated by all company systems has long since easily exceeded terabytes of data, representing an ill-structured, fragmented mass. The term "big data" has even emerged in the information field. It applies not only to information security, but to all areas that require huge processing volumes of structured and, more importantly, unstructured data to produce human-readable results. Collecting specific events from a limited set of devices is no longer sufficient, for example, from firewalls and intrusion prevention systems. You need to protect and therefore detect malicious or anomalous activity at the perimeter and directly within the corporate network, on resources that are closely or indirectly associated with assets. The detection paradigm has shifted from looking for the known to the unknown. It is, therefore important to collect, analyze and retain vast amounts of heterogeneous and seemingly unrelated information. Before an incident is detected, it is difficult to predict what data will be needed to investigate it. For example, it may be necessary to: reconstruct related network sessions - down to their contents and files transferred; locate related video surveillance recordings using events detected by these systems, compare information from storage and other physical security systems, and much more. Thus, the center's technical toolkit must be able to analyze this big data, becoming a single monitoring and investigative tool that integrates all the different technologies and can detect attacks or malicious activity from circumstantial evidence gathered from different equipment and information systems.

Figure 3 ***SOC technical architecture (example).***



THE PROPOSED MATURITY FRAMEWORK

Enterprise technological defense is the primary emphasis of this approach. Deploying a Security Operations Center (SOC) is crucial for businesses to meet and overcome cyber security threats. The original notion of a SOC was founded mostly on the reactive signaling of events. With time, the SOC has expanded its purview to encompass incident response, proactive research, and crime prevention. The growth and efficiency of a SOC are driven by its ability to get greater visibility into network traffic and operations, respond quickly to security incidents, and deliver reliable threat intelligence.

In light of the changes above and the IT auditor's position as a reliable service provider, it's important to disseminate best practices for evaluating SOC efficiency. Existing best practice frameworks (i.e., ISO2700, CobiT, or NIST-CSF) do not provide in-depth examinations of SOC operations, alignment, and maturity; hence, the SOC-MF was developed for this purpose.

In light of the changes above and the IT auditor's position as a reliable service provider, it's important to disseminate best practices for evaluating SOC efficiency. The SOC-MF was developed to facilitate thorough evaluations of SOC operations, alignment, and maturity. This was primarily necessitated by the requirement for existing best practice frameworks (such as ISO2700, CobiT, or the NIST-CSF) to accommodate such evaluations.

Framework Overview

Modeling the maturation of SOC capabilities is difficult. This is because SOCs use various technologies and provide vastly different services. But modeling is essential for measurement. Design Science was used to develop the suggested SOC model for maturity, which is an artifact that bridges the gap between theory and practice (Alharbi, 2020)(. SOC maturity model artifacts include the model and a self-assessment tool for quantitative evaluation. The SOC capability Maturity model was developed after considerable research of the available literature. All elements found in the literature were tested for occurrence in actual SOCs by conducting a survey among 16 participant organizations. SOC capability maturity model was developed using data gathered from the study. This model contains 4 domains and 25 aspects or elements and is shown in Table 1 below.

Framework Maturity Profile

To put it simply, cybersecurity in 2022 is unsustainable due to the ever-changing nature of the threats that must be dealt with. Only by upgrading to a more developed SOC model with numerous layers of defensive technologies will you have a fighting chance of survival.

Using the CMMI v2.0 maturity levels, we suggest a well-developed and systematic strategy for SOC. It's only possible to achieve cybersecurity maturity with a comprehensive suite of integrated and completely automatable protection, administration, and defense features. Figure 4 below shows the Security Operations Maturity level.

Table 1 ***The proposed SOC Model components.***

Domain	Aspects	
Business	Business Drivers; Customers Charter	Governance Privacy
People	Employees Roles and hierarchy; People management	Knowledge management; Training and education
Process	SOC management Operations and Facilities	Reporting Use case management
Technology	Security Information & Event Management (SIEM); Intrusion Detection and Prevention System (IDPS); Outsourcing	Security analytics; Automation and orchestration
Services	Security monitoring; Security incident management; Security analytics; Threat intelligence	Threat hunting; Vulnerability management; Log management

Figure 4 ***Security Operations Maturity level.***

Additional information on each Security Operations Maturity level, including the main technology and workflow/process capabilities that should be implemented, is provided in Table 2. Realizing each capacity will be accomplished in a myriad of unique ways. What matters is that you grasp the functionality of the capacity. We have also detailed the usual organizational and risk characteristics of each tier. This helps put security operations planning and evaluation into perspective. This provides additional context to support security operations maturity assessment and planning.

Assessing Capability Maturity

When the evaluation is finished, the scores will be displayed in a table and a graph in the SOC capability maturity model's findings section. The assessment's overall maturity rating is displayed graphically as a huge radar chart. Capabilities are solely evaluated based on their applicability to the provision of technology and services, as was mentioned before in this article. Disparities between the actual and ideal degrees of maturity are

Table 2 ***Security Operations Maturity level.***

Level	Security Operations Capabilities	Organizational Characteristics	Risk Characteristics
Level 0- Initial	None	• Focused on avoiding problems before they happen (using precautions like firewalls, antivirus software, etc.) • Logging is done in technological and organizational silos, with no oversight from a centralized location. • While there are indicators of threat and compromise, they are not readily apparent since no threat-hunting is taking place to bring them to light. • There is no standardized procedure for dealing with emergencies; instead, people step up to help one another in the heat of the moment	• Potentially stolen intellectual property • Lack of compliance • Ignorance of internal threats • Ignorance of external threat • Ignorance of advanced persistent threats (APTs) (if of interest to nation-states or cybercriminals)
Level 1- Basic	• The consolidation of log information and security events is required by law. • Legally required server forensics such file integrity monitoring and endpoint detection response (EDR) • A bare minimum of compliance monitoring and action	• Improved insight into threats targeting the protected domain but lacks personnel and procedures for practical threat evaluation and prioritization • Compliance-driven investment or have identified a specific section of the environment requiring protection • There is no standardized procedure for dealing with emergencies; instead, people step up to help one another in the heat of the moment	• Weakened compliance risk significantly (depending on the depth of the audit) • Assumed to be unaware of most internal risks • They are oblivious to most external threats. • Ignorant of Advanced Persistent Threats • Patently Stolen Material (if of interest to nation-states or cybercriminals)
Level 2-Defined	• Information logs and security events may be centralized and analyzed more precisely. • Forensics on specific servers and client devices • The Characterization of Environmental Risks in a Targeted Manner • Vulnerability intelligence processes that are reactive and manual • The automatic and slow threat intelligence process • First-order machine learning for prioritizing alarms and identifying patterns • Methods for initial monitoring and reaction are in place.	• Trying to do more with less and get better confidence rather than just checking off boxes • We now know that the majority of risks are going unnoticed within the company, and we are working to significantly increase our ability to identify and respond to the highest-risk threats. • Have explicit systems in place for monitoring and high-risk alarms, and allocated duties • have put in place a simple but formal procedure for handling incidents	• Superiorly tenacious and productive compliance stance • The ability to recognize insider threats is enhanced, albeit there may be some blind spots. • Accessible information on potential dangers from the outside world, with some gaps • often uneducated about APTs but adept at spotting their telltale signs and traces • Enhanced resistance to cyber assaults, except APTs and other specifically targeted vulnerabilities. • Extremely susceptible to attack by national governments

Table2 *(Continued).*

Level	Security Operations Capabilities	Organizational Characteristics	Risk Characteristics
Level 3-Managed	• Systematic log data and a centralized security event database • Forensics for all types of servers and client devices • Forensics on a certain portion of a network • Analytical and workflow integration of threat intelligence based on IOCs • Integrating fundamental correlation and workflow into a holistic view of vulnerabilities • Analytics of known threats using indicators of compromise and time to protect • Anomaly detection using targeted machine analytics (e.g., via behavioral analytics) • The process of monitoring and responding to threats is formal and well-developed, with standard playbooks in place for the most prevalent types of danger. • Automation of the workflows involved in investigations and preventative measures • Metrics for basic operational success: mean time to repair (MTTR) and mean time to diagnose (MTTD)	• have realized there are several high-impact risks the company isn't aware of • Have allocated resources to bolster the organization's capacity to identify and respond to all types of danger, and the quality of those procedures and personnel. • have invested in and set up a fully functional, staffed security operations and incident response center (SOC) • are doing a good job of keeping tabs on alerts and have moved on to proactive threat searching • Use automation to streamline their threat analysis and incident response procedures for faster, more effective results.	• Exceptionally dogged and fruitful compliance attitude • Despite such gaps, the capacity to discern insider threats has improved. • Information about external threats is readily available, however incomplete; yet, many people have a good eye for identifying the telltale symptoms and traces of APTs despite their lack of formal training in this area. • Resistance to cyber attacks has been improved, especially against APTs and other targeted flaws. • vulnerable to assault from foreign countries • Superiorly tenacious and productive compliance stance • Superior awareness of, and responsiveness to, insider threats • An excellent ability to detect and respond rapidly to external dangers • You can see APTs well, although there are some blind patches. • Extremely resistant to cyber assaults, save those employing advanced persistent threats (APTs) that aim to exploit vulnerabilities in specific infrastructure components. • However, the likelihood of early detection and prompt response has greatly increased.
Level 4-Optimized	• Comprehensive log data and a centralized security event database • Forensics for all types of servers and client devices • A complete investigation of a network • Intelligence on threats based on indicators of compromise and techniques used to compromise included in analytics and processes	• Are a prime target for hostile governments, hackers, and criminal gangs • Are under constant attack from any number of directions (physical, intellectual, social), and they • Service interruptions or breaches are unacceptable sign of organizational failure. • invests in the finest people, technology, and processes	• Identifying and countering all types of danger promptly • detect APT activity early in the Cyberattack Lifecycle and handle it strategically • Exceptionally secure against all forms of cyber criminals • The ability to endure and defend against an opponent on a nation-state level.

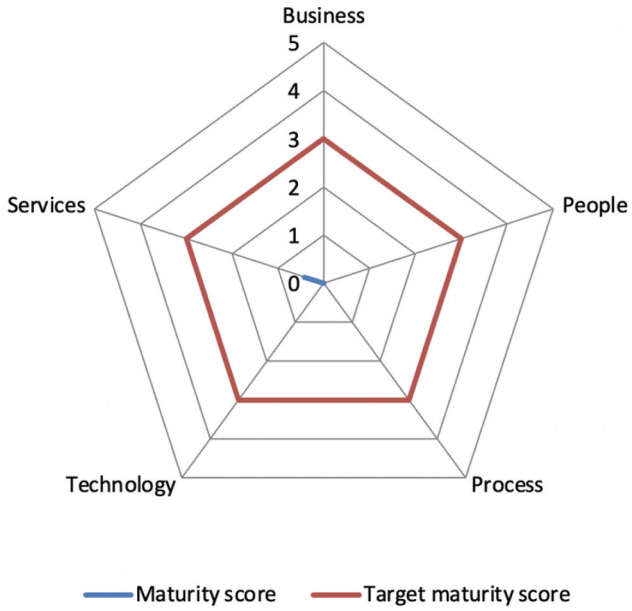
Table2 (*Continued*).

Level	Security Operations Capabilities	Organizational Characteristics	Risk Characteristics
	• Advanced correlation and automation workflow integration for comprehensive vulnerability intelligence • Intelligent machine analytics based on IOCs and TTP for detecting known threats • Machine learning and AI/ML-based behavioral analytics for comprehensive outlier discovery. • Processes for dealing with advanced threats that are well-established, well-documented, and fully mature, complete with standardized playbooks (e.g., APTs) • Physical or digital SOC in place, operational around-the-clock • Case management automation and cross-organizational cooperation • Workflows for both investigation and mitigation are heavily automated. • Common dangers may now be fully automated, from qualification through mitigation. • Enhanced operational MTTD/MTTR metrics and trend analysis	• Take a preventative approach to threat management and security • Have broad proactive capabilities for threat prediction and threat hunting • Have automated threat qualification, investigation, and response procedures wherever possible Have 24/7 alarm monitoring with organizational and operational redundancy.	

provided at the control level and as an aggregated score for each domain. Differences between actual and ideal maturity levels are presented at the control level and as aggregated scores for each domain. Figure 5 shows, for the different domains, the gap between the ideal and actual levels of development.

Figure 5 shows the specifics of each area, which may be used to assess performance. Weak facets of the domain have an adverse effect on the domain as a whole and should be worked on. The plan for improvement itself has to be crafted with a risk-based strategy in mind. One such low-scoring area is the business sector. Despite the technical domain's better score (compared to the business domain), it should be prioritized if it has a greater risk. Keep in mind that a lack of development in any area might become a problem in the long run. This danger might not show up right away but could develop over time. The SOC will be unaffected by the lack of a sourcing procedure for new workers as long as there are enough analysts. Still, it may eventually drive the SOC to adopt hybrid staffing models or complete outsourcing.

Figure 5 ***Detailed capability maturity scoring.***



For good measure, the SOC maturity model is consistent with the National Institute of Standards and Technology's Cybersecurity Framework (CSF). The five steps of this framework are "identify," "protect," "detect," "react," and "recover." The SOC maturity model does not include a recovery phase because of the SOC's minimal involvement in most recoveries. Each assessment question was checked for applicability to the NIST CSF and mapped to the most pertinent element for NIST CSF alignment. In addition to being included in the main download, this mapping may also be obtained independently from the site.

CONCLUSION

If properly used, SOC works very efficiently and significantly increases the effectiveness of information protection activities. At the same time, it is possible to include business continuity measures into the center's area of responsibility, thus creating a single point of control and application to comprehensively protect the organization from business interruptions, reduce their probability, and enable recovery. However, it is possible to go a little further and extend the area of responsibility of such a center beyond just information security to cover related areas such as technical security, physical security, consolidation of video surveillance data, control of equipment management systems (power, ventilation, fire-fighting equipment, and many others). As a result, an information security incident monitoring and response center grows into an organization's situational or crisis management center. Nevertheless, the article's approach also applies to such a global center.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the author(s).

ORCID

Yassine Maleh http://orcid.org/0000-0003-4704-5364

REFERENCES

Alharbi, N. (2020). A Security Operation Center Maturity Model (SOC-MM) in the Context of Newly Emerging Cyber Threats (Doctoral dissertation, The Claremont Graduate University).

Chamkar, S. A., Maleh, Y., & Gherabi, N. (2022). The human factor capabilities in security operation center (SOC). *EDPACS*, *66*(1), 1–14. doi:10.1080/07366981.2021.1977026.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1–147.

Crowley, C., & Pescatore, J. (2019). *Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey*. SANS Institute.

Edgar, T., & Manz, D. (2017). *Research methods for cyber security*. Syngress.

Exabeam (2019). SOC, SecOps and SIEM: How They Work Together. Retrieved October 22, 2022 from Exabeam website: https://www.exabeam.com/explainers/siem/the-soc-secops-and-siem/

Hevner, A., & Chatterjee, S. (2010). Design science research in information systems. In *Design research in information systems* (pp. 9–22). Boston, MA: Springer.

Hewlett Packard (2013). 5G/SOC: SOC Generations -HP ESP Security Intelligence and Operations Consulting Services—Business white paper. Retrieved from http://www.cnmeonline.com/myresources/hpe/docs/HP_ArcSight_WhitePapers_5GSOC_SO C_Generations.PDF

Hoffmann, M. (2014). How to build a successful SOC. *Presentation presented at the Protect*. Washington, D.C. Retrieved from https://h41382.www4.hpe.com/gfsshared/downloads-312.pdf

Jacobs, P., Arnab, A., & Irwin, B. (2013, August). Classification of security operation centers. In *2013 Information Security for South Africa* (pp. 1–7). IEEE. doi:10.1109/ISSA.2013.6641054

Johnson, B. G. (2014). Measuring ISO 27001 ISMS processes. 1–20. https://cdn2.hubspot.net/hubfs/163742/pdf_files/iso27001isms-kpi.pdf?t=1438891985360

Kelley, D., & Moritz, R. (2006). Best Practices for Building a Security Operations Center. *Information Systems Security*, *14*(6), 27–32. https://doi.org/10.1201/1086.1065898X/45782.14.6.20060101/91856.6

Maleh, Y., Sahid, A., & Belaissaoui, M. (2021). A maturity framework for cybersecurity governance in organizations. *EDPACS*, *63*(6), 1–22. https://doi.org/10.1080/07366981.2020.1815354

Maleh, Y., Sahid, A., Ezzati, A., & Belaissaoui, M. (2018). A capability maturity framework for IT security governance in organizations. *Advances in Intelligent Systems and Computing*, 735. https://doi.org/10.1007/978-3-319-76354-5_20

McKenney, S., & Reeves, T. C. (2013). Systematic review of design-based research progress: Is a little knowledge a dangerous thing? *Educational Researcher*, *42*(2), 97–100.

Meenan, C., & Laurens, V. (2015). Building a Next-Generation Security Operation Center Based on IBM QRadar and Security Intelligence Concepts. Presentation presented at the InterConnect 2015, Las Vegas. Retrieved from https://www.slideshare.net/ibmsecurity/building-a-nextgeneration-security-operation-centerbased- on-ibm-qradar-and-security-intelligence-concepts

Michail, A. (2015). *Security operations centers: A business perspective* (Master's Thesis).

Miloslavskaya, N. (2018). Information security management in SOCs and SICs. *Journal of Intelligent & Fuzzy Systems*, *35*(3), 2637–2647.

Schinagl, S., Schoon, K., & Paans, R. (2015). A Framework for Designing a Security Operations Centre (SOC). *2015 48th Hawaii International Conference on System Sciences*, 2253–2262. https://doi.org/10.1109/HICSS.2015.270

van den Berg, J. (2018). Cybersecurity for Everyone. In M. Bartsch & S. Frey (Eds.), *Cybersecurity Best Practices*. Wiesbaden: Springer Vieweg. https://doi.org/10.1007/978-3-658-21655-9_40

Van Os, R. (2016). *SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers*. Sweden: Luleå University of Technology.