# SOC-as-a-Service

**Florin Vidu**
National Institute for Research and Development in Informatics - ICI Bucharest
florin.vidu@ici.ro

**Abstract:** Enterprises face an onslaught of security data from disparate systems, platforms and applications concerning the state of the network, potential threats and suspicious behavior. Endpoint security, intrusion detection and prevention, security information and event management (SIEM), threat intelligence, and other security systems flood security teams with a lot of alerts and log entries and this is becoming increasingly difficult to manage.

With the number and sophistication of cyberattacks growing, some of these messages require urgent attention. But which ones? That's where a security operations center (SOC) comes in. Rather than being focused on developing security strategy, designing security architecture, or implementing protective measures, the SOC team is responsible for the ongoing, operational component of enterprise information security. Security operations center staff is comprised primarily of security analysts who work together to detect, analyze, respond to, report on, and prevent cybersecurity incidents. Additional capabilities of some SOC can include advanced forensic analysis, cryptanalysis, and malware reverse engineering to analyze incidents.

**Keywords:** Security Operations Center, SOC, Cyber threats, MSSP, SCADA, Firewall, IT infrastructure, cybersecurity, SOC-as-a-Service, Continuity, Human Resources, Stages, Build, Choice

## INTRODUCTION

The last decades have made a huge contribution to the development of the information society, bringing a number of benefits that cannot be ignored in any of the sensitive areas of an economy (Alfardan, 2015). The exchanges of data and the speed with which they are transmitted from one side to the other of the Earth have increased exponentially. All of these practically happen in a virtual environment, supported by the worldwide expansion of the Internet, both through the possibilities of terrestrial and mobile communication.

Not to be exaggerated, but it can be argued that we are in an era of technology where more and more emphasis is placed on data exchange and interoperability between national and international information systems and this reality is a major challenge. Cyber threats make an entity responsible for realizing that it needs continuous and comprehensive protection but this can be achieved either by designing / building its own Security Operations Center (SOC) or by using dedicated MSSP services *[Blokdyk, 2018a]*.

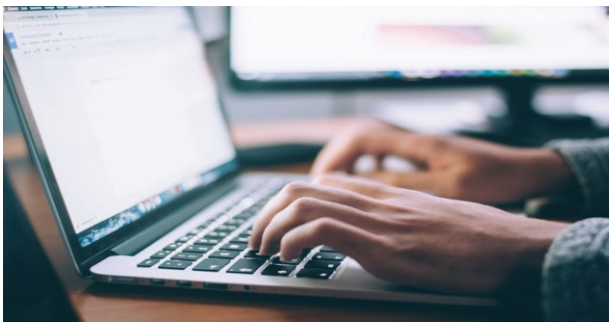

***Fig. 1:*** *Type of equipment in a SOC*

Regarding the first option, we had to face mixed challenges and sometimes difficult to overcome, because a SOC itself involves complex stages if we want to implement it and function sustainably in the long term under conditions of evolutionary adaptation, accomplishing all these in continuity conditions 24/7/365.

The second option is simpler for a client because it uses the services provided by a dedicated SOC, which means that the level of integration of technologies is much deeper than the own SOC option, including that the human resource is much more qualified and available with more lightness for continuity activities.

Returning to the context of evolution, it is noteworthy that at a level unimaginable a few decades ago, information technology has reached into all sectors of a modern economy, so today we can see that it has become commonplace for financial-banking transactions to be carried out in the online environment, for the payments of the invoices to be made from people's homes or even from the mobile phone while traveling on the street, so that an increasing diversity of forms can be completed remotely under conditions imposed to respect the right to the protection of personal information, etc.

It is inevitable, however, that these technological leaps of possibilities for massive data transfer and their manipulation should not be „accompanied" and with less honest intentions of intercepting and altering them, while pursuing different purposes that can leave industrial espionage or military, theft of civil data, theft of technologies and intellectual / industrial property rights and so on.

## TECHNOLOGY AS A WEAPON

When we talk about industry and high-level process supervisory management, we can mention Supervisory control and data acquisition (SCADA). This is a control system architecture comprising computers, networked data communications and graphical user interfaces(GUI) for high-level process supervisory management, while also comprising other peripheral devices like programmable logic controllers (PLC) and discrete proportional-integral-derivative (PID) controllers to interface with process plant or machinery. The use of SCADA has been considered also for management and operations of project-driven-process in construction.

Given that SCADA industrial control systems monitor and control processes from a multitude of critical industries and infrastructures worldwide (energy production, transportation and distribution, water production and wastewater treatment processes, agriculture, product processing food and chemicals, etc.), protecting against cyber threats in recent years is equivalent to preventing these essential infrastructures from disturbances, material damage and / or economic losses. If the magnetic, mechanical or analog elements, like monitor and control the system, are controlled by devices that communicate digitally, they can become the target of cyber-attacks. Most of the time, the risk of exposing a critical system to cyber-attack is underestimated (or misunderstood), which complicates the process of detecting, analyzing and mitigating such attacks.

***Fig. 2:*** *Flows of data*

It can be seen that the security of IT and communications systems has not developed in proportion to the degree of penetration of these technologies in various fields and in general in the social-economic life.

It is enough to remember that for a long time, IT specialists considered it sufficient to implement network-type Firewall equipment and an Antivirus platform at the IT infrastructure

level, their main focus being on ensuring functionality, security was not considered a critical process.

One of the main issues that arise in the context of cybersecurity is that the relationship between attackers and those who play the role of defenders is somewhat asymmetric *[Blokdyk, 2018b]*. One side of this problem is that the player who plays the role of the defender needs to identify and repair any potential vulnerability in their own systems exposed to the outside, but the attacker often needs to discover only a single vulnerability that allows them to penetrate the system or even the network.

In addition, there is that factor that cannot be easily overcome, generated by the reality that the very nature of the internet causes a potential attack to occur at any time, from anywhere in the globe and that most of the time it happens that the time elapsed between initial penetration and the complete compromise of the systems should not allow much time for the defender to react. The best example in this case is the penetrations manifested by ransomware, which are most often triggered immediately by encrypting files, this process continuing until a complete compilation of the entire IT eco-system.

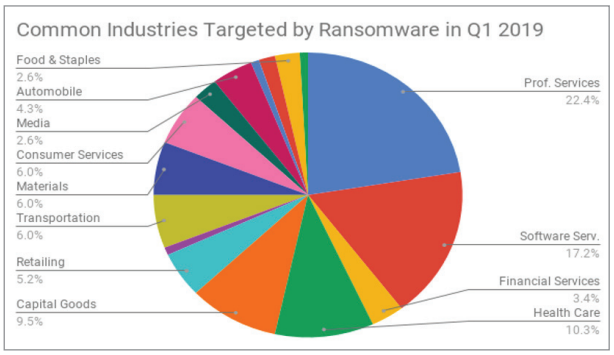


***Fig. 3:*** *Common industries targeted by Ransomware*

This reality has meant that SOC represents that form of natural response to the exponential growth of the types of cyber threats, the diversification of the forms and the sophistication in which they are designed to penetrate computer systems for different purposes.

It is easy to see that the gradual evolution of software and hardware technologies has allowed these technologies to turn into a two-edged weapon, because the complexity of the new software products has allowed the tools that serve to commit cyber-attacks to become increasingly sophisticated and flexible in adapting to their coping mechanisms, as they are thought by the big players operating in the cybersecurity market.

## CYBERSECURITY TECHNOLOGIES AVAILABLE

In other words, the threats from the cyber space continued to flourish and diversify, becoming more and more subtle and sophisticated. In essence, a cyber-attack is that form of intentional and unauthorized exploitation (of computer systems, networks and even data centers), through a malicious code in order to modify the computer code, data or logic. operation. The forms of destructive consequences range from compromising one's own data to stealing information or identity *[Blokdyk, G. 2019]*.

There are estimates that claim that, at the global level, there would be about hundreds of cybersecurity technologies, of different complexities, serving more or less complex purposes (civil or military), supporting some flexibility in updating and upgrading, etc. Of course, any of them at its own cost, which is primarily related to the degree of protection offered and the level of intelligence incorporated into these software products.

***Fig. 4:*** *Camera recording flows of data*

It is noteworthy that any software product that today is considered to be properly serving a customer, covering its current needs at a high

level, as a means of protection sufficient for the present moment, will arrive in a relatively short time to depreciate as a means of defense and can no longer respond to that primary need to combat cyber threats, as threats become more sophisticated, subtle, or new types of threats emerge. History shows us that there are already listed families of types of threats: Malware / Ransomware, Phishing, Trojan Horses, SQL Injection Attack, Cross-Site Scripting (XSS), Drive-by Attack, Denial-of-Service (DoS), Session Hijacking and Man-in-the-Middle Attacks, Credential Reuse, etc. *[Muniz, J., Frost, M., & Santos, O. , 2020]*.

An intelligent, structured approach, worthy of the context of the reality we live in, is to resort to the most capable forms of response that can be given in an integrated, flexible and resourceful way and for the future.

The Security Operations Center (SOC) is part of this class of tools for combating cyber threats and attacks. But such a modern tool involves a particular context, shaped by the need for hardware and software infrastructure as well as the appropriate human factor prepared and available 24/7/365.

It therefore raises the question of what options are available to any manager, a manager who among his attributions also those of has defending the interests of the entity he represents. [6] *[Phillips, R.,2018]*. As a particular remark it is possible for top management to be familiar with notions such as: Firewall and Antimalware / Antivirus, but it is extremely unlikely that they will be familiar with such notions as: *DLP*, *DDoS*, *Sandboxing NIPS / HIPS* and *IDS*, *EDR*, *EPP*, *Cyber Threat Intelligence*, *Threat Hunting*, *Digital Forensics*.

A first option a manager identifies is to be tempted to buy his own SOC. But such an approach is costly, because it involves significant costs for the purchase of hardware, software, licenses on the one hand, and on the other hand the cost that it can afford with a human resource as far as the SOC can operate, but with the obligation that it will need additional own personnel to ensure continuity in 24/7/365 regime *[Phillips, R., 2018]*. In addition, such a manager should have a very solid perspective so that he is able to lay the foundations of a structured approach, starting from the identified needs, namely the planning, implementation and efficient operation of a modern SOC, flexibly adapted to respond to the need of the served entity.

A second option can be justified from a large to very high level of an entity/enterprise. For a small/medium entity, such an option is profoundly unjustified economically and with little chance of being sustainable in the long term, when potential threats become more sophisticated, more innovative and stronger. When we consider a small/medium entity and the cost reporting must be taken into account that it is the sum of those amounts that are necessary for acquisition /construction, salaries, maintenance, use and periodic training, mainly the so-called recurring costs, including potential future costs with the purchase of new technologies that respond to other types of threats, etc.

## SOC-AS-A-SERVICE

However, such a manager can opt for an alternative to the traditional SOC, but with significantly lower costs with a much greater sustainability over time, at some flexible and upgradable parameters over time.

This alternative is represented by SOC-as-a-Service. That is, that type of approach in which the own constants are clear and respected over time (the need for protection and security of the entity in the long term in the face of present and future threats) but the instrument (as a line of defense) is outsourced, while ensuring continuity (in 24/7/365 regime).

Such a SOC-as-a-Service solution must be regarded as a complex environment in which a multitude of distinct security instruments contribute to creating that barrier that will be between the beneficiary entity and its external environment. Basically, a team of specialists, dedicated to a particular purpose, monitors a set of consoles on which are displayed parameters related to security events and/or threats identified *[Phillips, R.,2018]*.

From another perspective, we are talking about a complex, highly integrated mechanism, capable

of responding to increasingly sophisticated diversified threats, blocking from the early stages of penetration attempts. This mechanism being operated by specialists, continuously trained professionally and who have access to much deeper knowledge bases, thus being able to appreciate in real time the type of threat, subsequently cataloging the priorities and escalating the problems to the higher levels.

For any of the beneficiary entities, this represents, on the one hand, an advanced protection for threats but on the other with minimum levels of cost, because the costs, as a reflection of the complexity of the activity processes, the aspects of technological infrastructure and with advanced human resources are the burden of the SOC holder.

For the SOC owner, the costs are significant, both in terms of the necessary hardware and software purchases, as well as the operating/ recurring costs, the periodic replacement of equipment, updates and upgrades, additional licenses as well as professional human resources.

## WHAT IT MEANS TO MAINTAIN A SOC

Basically, we can talk about real professional challenges in maintaining a SOC in the long term capable of dealing with any new threats, because we are talking about continuous training for operators/responsible, mainly generated by the changes in the subtleties of the attacks and the technologies used for penetration attempts.

From the point of view of the concept of SOC, there are several levels to which it can relate the interaction of the environment: technology, processes and people.

At a technological level we deal with endpoint, data flow, network monitoring, threat information, forensic analysis, incident detection and its management.

As processes had to do with distinct stages: preparation, identification, isolation, eradication, recovery, a new lesson learned.

As for the people, the specialized human resource, we deal with continuous activities of formal training, acquiring experience in the workplace, a specialized training offered by the technology producer, an internal training on working procedures.

***Fig. 5:*** *SOC*

From the point of view of the services of a SOC they are focused on ensuring the cyber security protection of the clients, through specific activities of monitoring, detection, alerting, reporting and reaction to the security problems.

Basically, it is envisaged that SOC should offer its clients that efficient barrier against cyber threats, respectively of offering that capacity sufficient for extremely fast detection and reaction, in order to mitigate the threats that endanger the activity, with serious repercussions, and major financial and patrimonial losses.

In a broader sense it can be said that the services offered by the SOC define the whole of the Security operations, in order to respond to the emerging and ongoing cyber threats.

From a human resource perspective, SOC services are provided by a dedicated team of specialists who monitor networks, servers, devices and other devices to protect sensitive data and comply with government regulations.

From a technological perspective, SOC uses a combination of technological solutions and a series of automated processes (Robot Process Automation) to permanently monitor and analyze the activity on networks, servers, applications, websites and other systems, operated by specialists in the field of cyber security.

***Fig. 6:*** *Data analysis*

As an infrastructure resource, it is possible for SOC technology to collect in a private cloud, data about events and security records through data flows, and other methods, so that data can be correlated and analyzed to accurately identify and counter threats and security incidents.

From the client's point of view, the operations are relatively simple, considering that cyber security services are provided through specialized equipment, installed at the beneficiary's premises and include the following types of integrated systems (operating systems and applications) for protection against cyber-attacks.

However, returning to the concept of SOC, whether we are talking about its own variant or the more complex variant represented by MSSP, the concept itself has several key elements.

Initially, these SOCs were designed and reserved for large organizations that had the resources necessary for their creation, implementation and operation, respectively the organizations in the government, military, national security, transport and financial-banking services fields *[Thomas, A., 2017]*.

As a rule, those in charge of security operations, as specialists in information technology, could decide to *centralize* ***the whole*** or ***parts*** of those activities in a form of SOC, considering the purpose of improving the maturity of their own security practices *[Thomas, A., 2017]*.

It can be observed, however, that this activity, as a process, was and still is dependent on the level of knowledge and experience and expertise of those specialists. Know-how, lessons learned and experiences gained are decisive factors.

But trying to decipher the concept we can start from ***the perspective*** by which we refer to the basis of a ***structured approach***, starting from the identified needs, namely a *planning*, *implementation and efficient operation* of a modern SOC, *flexibly adapted* to meet the needs of the served entity.

It is recommended that the management of an entity should be aware that the construction of a modern SOC/MSSP must start from several *premises*, understood as comprehensively as being in fact some ***preconditions*** which, as I already mentioned, are directly related to distinct categories: *people*, *processes* and *technologies*.

Globally, regarding these categories, we observe that all are important in their own way and all raise challenges in front of the specialists who are called to design and build modern SOC/MSSP systems, capable of proactively responding to different types of threats but under certain conditions of lower costs and with flexibility prospects in the face of new threats.

Thus, the rationale emerges that such circumstances inevitably lead to the first stage of the entire SOC process.

Usually, this first stage is the ***declaration/ definition of the problem***, respectively the crystallization of the information that outlines the problem so that a primary identification of its borders is ensured, considered in fact as some identified limits of the problem *[Thomas, A., 2017]*.

The boundaries, as such, once identified will directly contribute to the definition of the purpose.

It is essential, however, that such an activity be approached in an intelligent and not chaotic form, or tributes to customs or even to old principles, as a mere reflection on professional activity.

Human intelligence, embodied in its form of experience and professional expertise, will implicitly lead to flexibility in conditions of permanent reduction of the costs of implementation/operation.

Why is intelligence essential to such a sub-process? The mere fact that the purpose is clearly defined and proactively oriented will bring ***results*** in the medium term, but especially it is desirable to be long term.

***Proactivity***, in its paradigm, means to be anticipated in a real and fair way in a series of future prospects, but in conditions of cost reduction. It goes without saying that proactivity is one of the pillars on which the flexibility of a system is supported.

It is undoubtedly desirable for a SOC/MSSP system designed today to respond fully and immediately to the threats currently identified.

But it is even more desirable to be more adaptable to the future, more or less imaginable, as a form, at the moment.

## CONCLUSION

In conclusion, going further with this way of deciphering the concept, it is important to mention that in the thinking activity of a SOC/MSSP it is essential to use a *guiding framework*, as it is not intended that such an activity be done chaotically, or without a well-structured logic, as well as validated by previous positive experiences.

If we look at things from a particular angle, we can notice that threats can be categorized as distinct threats, depending on typologies and consequently interpreted as such. In fact, the respective threats are generated by entities that act independently and have a certain limited level of knowledge.

It is important, however, that the mechanism of protection against these threats should be intelligently designed keeping in mind the proactivity, adaptability and flexibility.

It is therefore self-evident that this guiding framework will have to have several clearly identified ***stages***.

In the logic of things, it can be noted that these are distinct elements, represented by *the pre-aggregation activities of the information*, *the planning activities*, *the implementation activities*, *the operating activities*, *the improvement activities*.

However, these will be permanently accompanied by activities designed to limit the risks and possible skids.

In *the first stage*, *the pre-aggregation activities of the information* are indicated to find those sub-processes that by their nature will contribute decisively to the success of a modern SOC/MSSP *[Thomas, A., 2017]*. These sub-processes, sequential by their logical nature, consist of:

- *analyzing and validating the motivations and directions chosen initially;*
- *the requirements and constraints of a SOC;*
- *identification of any need for help/external assistance;*
- *information overlap, dissemination and matching within the purpose;*
- *building the SOC business case (as a business house).*

The second stage is more evolved and requires on the one hand a more consistent intellectual effort and a greater volume of work but on the other hand it also requires a deeper knowledge mix on various fields, doubled by an ability to anticipate certain future evolutions, meaning to create the basis for the proactivity of the SOC/MSSP system.

In this context, it is compulsory to find those sub-processes that directly contribute to defining the architecture of the entire SOC/MSSP system envisaged as a goal.

In short, the sub-processes of this stage are also sequential and will require a much greater combined effort, because here ***a plan will have to be made***, respectively:

- *defining the functionalities of the SOC system and the purpose of responsibility;*
- *designing the organizational structure of the SOC system;*
- *defining the SOC model, hybrid or not;*
- *the organizational links of the SOC system.*

It is obvious that from the logical point of view, the third stage corresponds to the implementation phase of the SOC, which would be described as actually:

- *implementation of the SOC process framework;*
- *insertion or integration of SOC instruments;*
- *make up the SOC team;*
- *the project for the effective implementation of the SOC.*

The *fourth stage* follows, that of the actual operation of the SOC, which translates into clear, distinct activities, which are in a collaborative environment, of which the most important can be summarized in:

- *the operation in continuity regime 24/7/365;*
- *labor management, available in the context of SOC;*
- *cooperation with a possible MSSP;*
- *measurement of SOC performance indicators.*

It is obvious that if it is desired to maintain a positive trend of evolution of the SOC, respectively of continuous adaptation to the realities of the new threats arising in the cyber environment, logically the following is the *fifth stage*, through which it is indicated that the

*improvement of the SOC* will be followed and such activities usually involve improving SOC to respond to new types of threats, by:

- *evolution and expansion of SOC;*
- *proactively starting the pursuit of new threats;*
- *removal from the classic model of reporting only alerts;*
- *implementation of automation and orchestration of instruments;*
- *introduction of deterrent techniques;*
- *the eventual evolution towards the production of own instruments/intelligent methods of detection/response;*
- *extension of the use of advanced analysis tools;*
- *continuous maintenance of SOC performance testing;*
- *improving the maturity of SOC.*

But there is also a stage, collateral, concomitant with any of the steps described above, namely the *mitigation stage of risks and system failures*, which in itself is a large process consuming human and time resources.

So, starting from the ones described above, two questions can be asked:

***HOW EFFICIENT AND JUSTIFIED IS THE CHOICE TO BUILD YOUR OWN SOC?***

and

***HOW EFFICIENT AND JUSTIFIED IS THE CHOICE OF THE SERVICES OF A DEDICATED MSSP?***

**REFERENCE LIST**

Alfardan, M. M. A. N. M. G. M. J. (2015). Security Operations Center: Building, Operating and Maintaining Your SOC (1st ed.). Amsterdam, Netherlands: Amsterdam University Press

Blokdyk, G. (2018a). Security as a service : 5STARCooks

Blokdyk, G. (2018b). Security operations center: Complete Self-Assessment Guide. Zaltbommel, Netherlands: Van Haren Publishing

Blokdyk, G. (2019). Network Security Operations Center A Complete Guide - 2020 Edition: 5STARCooks

Muniz, J., Frost, M., & Santos, O. (2020). The Modern Security Operations Center (1st ed.): Addison-Wesley Professional

Phillips, R. (2018). Cyber Security (1st ed.). Abingdon, United Kingdom: Routledge

Thomas, A. (2017). Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices. USA: Arun E. Thomas