```
ring:                used; the default culture is [en-US]:
 format string:              11876.54
' format string:             11,876.54000
E5' format string:           1.187654E+004
                             1.18765E+004
nfo object for [nl-NL] is used for the IFormatProvider:
t string:                    11876,54
rmat string:                 11.876,54000
rmat string:                 1,187654E+004
NumberFormatInfo object with digit group size = 2 and
igit separator = '_' is used for the IFormatProvider:
'N' format string:           1_18_76,54
'E' format string:           1,187654E+004
Press any key to continue . . . _
```

Preliminary Technical Analysis of the Establishment of Information Security Operations Centers in Companies with Critical Energy Infrastructure

Content

Preliminary Technical Analysis of the Establishment of Information Security Operations Centers (SOC) in Companies with Critical Energy Infrastructure

*Author: Tomas Pleta, Fellow, Doctrine and Concept Development Division,
NATO Energy Security Centre of Excellence and PhD student at Vilnius Gediminas Technical University*

*Supervisor: Ana Gogoreliani, Subject Matter Expert, Doctrine and Concept Development Division,
NATO Energy Security Centre of Excellence*

2022, Vilnius, Lithuania

INTRODUCTION

The purpose of this handbook is to present an extended evaluation, analysis, presentation of standards and correlations in the field of cyber / physical security of critical energy infrastructures. In general, critical energy infrastructures are those infrastructures that provide goods, the systems and subsystems that are necessary and are vital for the functioning of society, health, physical protection, and security, economic and social well-being of citizens. Energy management and distribution networks, for example, banking infrastructure, water supply network, mobile telephony networks, airport systems, all of the above are critical energy infrastructures which are directly related to the operation of further industrial and automated systems, and play crucial role in the smooth running of states and their services. Critical energy infrastructures at both physical and digital levels including security against cyber-attacks are interconnected through complex mechanisms. This is an advantage but also a disadvantage, an advantage because all operations are done automatically and one system recognizes the other, a disadvantage is because in case of cyber-attack on some part of the whole system it will cause chain problems in other interconnected industrial systems and networks, consequently the smooth operation of a critical energy infrastructures will be directly affected. Identifying vulnerabilities, implementing security policies, training, updating systems, and even removing urn-necessary systems that do not meet current security and operational needs will be a lever to avoid future cyber risks. The faithful application of cyber security policies in combination with the proper employee training, correct network and devices configuration, and physical security, will lead to the prevention or significant reduction of the risk to a tolerable level.

Risk Management is still the most popular method for assessing security and risk needs in both the short and long term. The Risk Management process is necessary to set priorities by prioritizing security priorities in an infrastructure to identify vulnerabilities and make future forecasts using parallel forecasting models, taking into account data and information from both open source and existing threats to critical energy infrastructures, which however were or were not successful. Every critical infrastructure with an enterprise network and related assets needs IT risk management, which is controlled by the information technology (IT) department. However, data security needs may increase until a dedicated security operations center (SOC).

The main benefits of SOC are its increased security by constantly scanning the network for threats, weaknesses and fixing them before they turn into critical issues or incidents. In addition, the SOC consists of tools and processes such as security information and event management systems (SIEMs), breach and instruction detection, firewalls, and probes. Taken together, it all focuses on daily operational security and is less about designing or developing security strategies and architecture. Beyond to increasing security, SOC has additional benefits:

1. *Reduced costs* - having one security team helps in less overlap in job duties. In addition, it helps to avoid fines and other penalties due to violations of data security regulations.
2. *Centralized activities* - brings together IT security functions between different workgroups and locations into a single team, to improve collaboration advantage shared knowledge and experience to optimize results. The SOC serves are a single point of contact for coordinating security activities and disseminating key information and policies.
3. *Increased prestige* - ensures data security, thereby increasing prestige.

This Handbook was written to help establish SOC and proper management processes in SOC of an electric power utility, gas, oil, green energy, health, transport, food, chemical & nuclear energy, space & research or other industrial systems. It is intended for cyber security policy makers and senior plant engineers working in the control rooms monitoring industrial control systems processes and operations, also this handbook is useful for the peculiar interests of the plant engineers who is less concerned with information but more with insuring the security, reliability and performance of a physical process such as generating and distributing electricity, green energy, gas water, oil, health, transport, food, chemical & nuclear energy, space & research information services to customers. This Handbook is mainly aimed at NATO infrastructure, which are nuclear protection, electricity generation and management, weapons systems industry and quality assurance, industrial integrity in industrial environments, protection of automated industrial systems in NATO member states, critical NATO infrastructure interacting with industrial facilities in other NATO member states, protection of any critical energy infrastructures operating in disputed operating environments.

PART I: METHODOLOGY AND MODULE

Cyber Security Management for Critical Energy Infrastructure

Computer networks undoubtedly offer great and important possibilities of interconnection, automation, decision making, scalability of various electronic devices and computer systems, which are nowadays everywhere and of course are exist in critical energy infrastructures. As networks evolve, upgrade and add smart devices and computer systems, the security of networks and the inadequacy of the information transferred on it, is significantly reduced, leading to questions and concerns about the integrity and protection of processes. Every computer unit, and generally every device connected to a network, of course means any device that can receive an IP address, and is able to communicate with the rest of the network or communicate with other electronic devices, whether it is a working station or industrial control system (ICS) is able to collect, store, exchange information with each other through a network that implements a security policy which, depending on the criticality of the infrastructure, implements the corresponding security policy. The industrial control systems (ICS) should be included in a discussion, along with the IT CIA priority list. At ICS Safety, it is the first priority followed by confidentiality, integrity, and availability. [1] There are many good reasons both IT and ICS security professionals should sit at a table together, exchange information, and listen each other. What IT security professionals are saying should get the attention of ICS security professionals and vice versa.

The concerns of Chief Information Security Officers (CISO) of critical energy infrastructures due to their nature are understandable; they have a lot to learn about industrial cybersecurity. They need to appreciate what the engineers are doing which to monitor and control a physical process, as the information and processes transferred through their data network of critical energy infrastructures are vital, as information on the operation of systems, automated systems, sensors, actuators, etc. The security problems observed in critical energy infrastructures networks are interlinked. Because, the use of remote management consoles for computing systems and digital infrastructure that are at critical sectors raises the level of threat to security, the operation of the infrastructure itself and the integrity of the information.[9]

A secure network in critical energy infrastructures should implement the following entities:

- *Authentication of information and devices, every device that is connected to the network and receives an IP address as well as an information system, even the use of a computer application must certify its authenticity and reliability. Special authentication mechanisms must be in place to ensure that each entity within the infrastructure operates in accordance with operating rules and infrastructure security policy. In this way, "**impersonation**" type attacks are significantly <u>reduced</u>, ensuring the security of the information circulating in the network as well as the security of the use of other systems within the infrastructure. One might wonder, why does an installed application need certification, and how could its use be changed? A computer application is the basis for achieving access control, assignment of management rights, application user co-responsibility and responsibility. The certification of information* *and devices can be done in various ways, such as indicatively mentioned using* ***NFC smart cards, DNA, Personal Identification Numbers, Voice Recognition, e-signature, etc****. As for smart devices, they can be authenticated using* ***passwords, cryptographic authentication systems and security mechanisms for identifying entities*** *by applying from one-way authentication to two-way-authentication.*

- *Control of network access and computing systems to critical energy infrastructures must include certification and authentication control mechanisms for protecting connections between network nodes and the data transferred through it, including databases. The security policy clearly defines the level of security as well as the ways and methods of certification and authentication of each unit located within a critical energy infrastructure.*

- *The information, process and device security policy applied to a critical energy infrastructure, is defined by a decision of the general manager of a critical energy infrastructures, is distributed to all involved internal and external bodies, including employees. It is reviewed at regular intervals and periodically every time significant changes are made to it, in order to ensure its complete completeness and effectiveness. The information security policy defines the duties of the staff and the internal / external bodies involved for the operation and maintenance of the systems. Clearly defines the level of security of the information and processes transferred on the data network, as well as the level of access of each user to the information. Only authorized users have access to this information and with the appropriate access rights to that information. The protection of data and information that transferred on the network infrastructure is determined by strict restrictions on the management and control of information per department and not collectively, policies are defined and restrictions are applied per department, the so-called "****Access Control Policies****" for which cryptography is often involved.*

- *The integrity of information, data, and operations is a very important goal, which is why security policies adequately determine the security actions and levels to be implemented. Creating, modifying, and deleting data from unauthorized users or even from unauthorized applications should be excluded whether this attempt is made during the transfer of information or during the storage of information or subsequently. It is very important in critical energy infrastructures for example energy management that information systems receive the right management commands for the smooth operation of the infrastructure. For data and information integrity are often applied encryption in different domains and different methods, for example, hashing, and database encryption systems.*

- *User certification combined with a high level of education and training significantly reduces the likelihood of digital intrusion into a critical energy infrastructure. The authenticity of information and data that in critical energy infrastructures is this kind of information is very important, the human factor plays a decisive role and they are two interconnected entities that for a high level of security must function harmoniously. Human resources must have a sense of responsibility for their handling and be tolerant of imputation, as critical energy infrastructures must be treated differently from a simple organization.*

- *Critical energy infrastructures communications networks should be readily available, free from loop "**Loop Free**" recycled data as well as free from unauthorized entities and attacks, such as **DOS, SYN,** and **Brute force** attacks. Resources of communication networks should always be available to perform critical energy infrastructures functions, for the purpose it is very important to monitor the network and services, which is also mentioned in the security policy applied to a critical infrastructure.*

- *Disaster Recovery Plan, disaster recovery is a set of policies and procedures that aim to ensure the recovery or smooth running of a critical energy infrastructures after a disaster, whether is physical disaster or cyber-attack. Physical disasters include earthquakes, floods, fires, man-made disasters, and malicious acts. While cyber disasters include system breaches, machine malfunctions, interception of processes, execution of infected code and exclusion of electronic services and functions.*

Critical energy infrastructures are complex systems that combine many functions, several of them are automated which rely solely on the right configuration should clarify the following:

- *Information that is on the network of a critical energy infrastructures that is then stored, the definition of access that network users will have, whether physical or remote, how they can be accessed outside of an accessible infrastructure or not, how to apply encryption or other methods of protection.*

- *Controlling the access of infrastructure users, which user has access to where, at what level and with what rights.*

- *Protection of data and information transferred within the network, any form of data, including personal data, whether relating to management data of machines and other digital devices.*

- *Creating a secure isolated information and data exchange network, a network where personal data will be added and infrastructure management and control data will be analyzed.*

- *Bad use of data network, poor configuration of devices and peripherals very often leads to problems. Unexplained loops are created on the network, available resources are reduced and the network becomes vulnerable.*

- *Continuous monitoring of the data network and anomalous Processes, what services used, the logging of events, running processes, and the correct sequence of the security policy that must be implemented in critical energy infrastructures is the best response to any kind of attack on the network. With the monitoring method, potential threats are quickly identified and isolated before they reach the internal network or hinder the smooth operation of an infrastructure.*

- *Critical domain passwords as well as private / public user-system authentication keys should be kept in an inaccessible part of the network, away from unauthorized users, as specific staff according to the applicable infrastructure hierarchy access them. It is very important that the encryption information is kept confidential; any interception would lead to interception of information, modification of stored information, modification of information during their transfer, even suspension of systems operation.*

- *Industrial Internet of Things (IIoT), The Industrial IoT is a huge ecosystem consisting of sensors, actuators, HMI, edge devices, cloud applications and services, algorithms, and other components that need to work together. This convergence is continuous and imperative. Real-time connectivity is essential for performing critical processes, as well as for collecting and analyzing data from machines.*

- *In critical energy infrastructures used "***Handshake Configuration***", which means that one application, computing unit, smart device, and any device that connects to the infrastructure network and obtain an IP address uses some authentication method to communicate with another applications or a general entity within a critical energy infrastructures, thus ensuring the smooth and confidential exchange of information and data in critical energy infrastructures, for example used in the* ***Industry 4.0****.*

Designing a data network on Critical energy infrastructures is an important part of the process leading to the design, acceptance testing, and exploitation of an industrial operation. Proper design of a data transmission network in critical energy infrastructures is the key role for both its smooth operation and its security. Network design however understandably focuses on the above entities. Critical energy infrastructures is a critical area of activity, which includes the creation of a different communication structure, which includes, sensors, actuators, artificial intelligence, smart applications, complex network architectures with special topologies, special applications, special network rules, specialized specifications and special standards, cryptography and communication protocols, which together contribute to the smooth design and implementation of high technical security standards and networks. [2]

Usually, the design of a network in critical energy infrastructures starts with a **top-down analysis** where the **conditions, priorities, operational functions, goals, security policies** are defined, and finally how the network will work when it is implemented. **Objectives, implementation planning and security policy** are defined based on some security standards and some customizations are performed on them. The analysis of the objectives and the conditions, help significantly in the correct design of the network where the rules and the type of network that is ideal for the infrastructure are determined. [10] The network design objectives in conjunction with the required security policies are crucial in terms of the choice of technology to be used after both the objectives and the requirements in both security and performance have been previously analyzed and identified. The design of a network in critical energy infrastructures presupposes the collection of operational and operational objectives of the infrastructure, such objectives are defined below.

- *Physical goal analysis.*
- *Physical security.*
- *Functions.*
- *Activities.*
- *Operating units.*
- *Infrastructure structure.*
- *Requirements for communication.*
- *Information systems*
- *Security.*

The stage of **analysis, identification of requirements, and needs** is the main point. The above three entities are very important, information is collected regarding the actual requirements and needs and the proper design of the network. The above three entities include Actual Requirements, Communication Requirements, Applications, Modules, Interface Methods, Nodes, Servers, Management Modes, and Network Security. As it is understood, the whole process is not a simple and short process, due to the criticality of the infrastructure, its smooth operation, the determination of the right level of security but also the correct logging of process needs and requirements; it is a time consuming and complicated process. The success of proper network design should combine speed, reliability of information transmission, be adapted to the needs of the infrastructure, provide uninterrupted functionality and a high level of access quality. [3]

Certainly, designing a secure and operational network in critical energy infrastructures is a challenge, because its design presents challenges in terms of **strategy, speed, reliability, functionality, and safety**. Network design should include procedures and techniques for **efficiency, confidentiality, functionality and security**. In addition to the above challenges, there are also telecommunications challenges, which must be taken into account. [12] One of the most important challenges is the selection of the right telecommunications media that are able to meet the needs of the infrastructure now and in the future, taking into account the technological omissions while expanding the needs of the network taking into account the future needs for communication and managing larger volumes of data without deviating from infrastructure objectives. [4]

Access Control in critical energy infrastructures is characterized by **the flow of materials, the flow of energy and finally the flow of information**. Monitoring the flow of information is the main goal of infrastructure control as integrated systems and raw material management are performed within an infrastructure. For the proper management of information require a critical energy infrastructure to be enriched as much as possible with digital systems that have been pre-decided and approved during the design phase of the infrastructure communications network, special emphasis should be given to those systems that regulate and calculate operating variables of production systems. [13]

The term access control describes the methods and technological solutions used for the autonomous operation of systems located in critical energy infrastructures. Depending on the composition of critical energy infrastructures in terms of the purposes of its operation, there are three terms, which can be classified critical energy infrastructures.

- **Continuous process infrastructure:** *In this category are those infrastructure that use in their materials products for production which are like liquid material, that is, they are in liquid form, such infrastructure are the power generation units and the refineries.*

- **Discontinuous Process infrastructure:** *are the critical energy infrastructures of a country whose equipment has the ability to change the operation of the infrastructure to create a different produced resource; such infrastructure is the infrastructure that produce mines.*

- **Batch Process infrastructure:** *They are the infrastructure, which for the production of specific products a specific sequence is performed and specific processes cannot be changed. The process of eliminating production is closely monitored at all stages. Such infrastructure is the infrastructure for the production of medicines.*

A security hole in a production system may be the backdoor of an import into a critical energy infrastructures system. The operating variables of the systems should follow certain specific security policies always according to their degree of operation. Security in industrial control systems is a top priority and it is a significant challenge to ensure information integrity, proper operation, and cyber security. Due to the criticality of infrastructure and their direct relationship with governments and policy-making systems, they are increasingly targeted by cyber-attacks, which requires a specialized approach in the field of security and implementation of integrated action plans, as well as common operational plans. The need for specialized security and protection against cyber-attacks is confirmed since 2016, which have had the second cyber-attack on Ukraine's power grid, NotPetya, Trisis in 2017 and Norsk Hydro in 2019. Also, according to Industrial Cybersecurity Threat Briefing, in 2016, where it states that 34% of critical energy infrastructures reported security incidents more than twice a year. In the same year, a survey by the SANS Institute was published which states that 32% of critical energy infrastructures have fallen victim to some form of cyber-attack without mentioning the numbers, the most important finding of the survey is that 42% of these attacks, the security officials were unable to locate the source of the attack. At 24%, attacks on critical energy infrastructures are significant, compared to 15% in 2015. This marks the growing course of attacks and the concern that prevails in this area. The survey further details the data and states that 61% of the attacks on critical energy infrastructures came from the external network and not from the inside, while 42% are attacks from inside the infrastructure, which are due to either sabotage or human mistakes.

Most of the failed attempts to breach critical energy infrastructures systems are reconnaissance attacks, these attacks are not intended to breach the system but to scan the target infrastructure network to identify security vulnerabilities and map the data transmission network. This information is then analyzed by various cases, such as, for a further successful attack, for the creation of automated tools that take advantage of specific security vulnerabilities and the sale of this information in interested third countries. [5]

Cryptanalysis is undoubtedly an interesting branch of science dealing with cryptography; critical energy infrastructures must take seriously the encryption algorithms they choose to use for the encrypted communication of their systems. Critical energy infrastructures are not directly affected by cryptanalysis as an attack on encrypted communications and operations systems presupposes other stages of attack and information gathering, which involves compromised systems and the interception of encrypted information. A hacker to possess encrypted material on critical energy infrastructures means that security systems have been severely compromised and there is a lot of intrusion into sensitive information, but this is an extremely difficult case as critical energy infrastructures security systems have excellent resilience to cyber-attacks, implement security policy correctly and carry out analysis to predict and address future cyber threats, at least this applies to European critical energy infrastructures. Even if a hacker somehow steals encrypted material, which has been encrypted with a secure encryption algorithm in conjunction with today's computational speed, it will take hundreds of years for a cryptanalyst or a hacker to be able to analyze the encrypted content.

A critical energy infrastructure differs from an organization, in levels of, digital security, physical security, operation, installations, communications networks and automated systems. Critical energy infrastructures are complex infrastructure that, due to their production, produce products, which are in various forms, which can also be intangibles, forms such as energy. The control procedures play an important role in an industrial unit both for its proper and uninterrupted operation and in the proper management of the control systems of the unit. The complete and correct control process aims at timely troubleshooting and correct decision-making such as for example the proper selection of input elements in one system for the correct operation output in the other connected system; this implies the correct performance of the system and the creation of correct result. [6]

Undoubtedly, the best security strategy is to prevent the attack by applying various models of future predictions and applying security methods before the hackers test the security of some point of the infrastructure. Therefore, the following will be considered a management model targeting Critical energy Infrastructure protection, which is the continuation of the model developed by Limba et at al. (2017). The description of the model is not performed in-depth, but instead offers a general overview of its core components and the relationship between categories, along with some elucidation of the classification choices and motivations. Other sources that have been considered in the redaction of this model are previous works of the authors, including the articles *Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases* (Plėta et al., 2020), *Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania* (Tvaronavičienė, Plėta, Casa, & Latvys, 2020), and *Cyber effect and security management aspects in critical energy infrastructures* (Plėta, Tvaronavičienė, & Casa 2020). In terms of the development of the concept of security and awareness within an enterprise, other articles that were useful for the research were *Training in shaping employee information security awareness (*Stefaniuk, 2020) and *Organizational security culture in small enterprises: a case study* (Gierszewski, 2020).

The concept of cybersecurity considered for this model follows the *CIA Triad,* which is comprised of three major objectives: *confidentiality,* meaning the protection of sensitive information from unauthorized access; *integrity,* meaning the protection of data from unauthorized access, and finally *availability*, meaning that the systems' mechanisms are available in emergencies (Forcepoint, 2020). Having this in mind, it is important as well to clear that the structure and core principles of the model will be appliable to every type of CEI to achieve cybersecurity, and considers the advancement of new technologies as an integral part of the model. However, the model as well considers the *n-1* principle for technology: although the model promotes the newer technology for ICT systems to rely on, it is considered better to rely not on the latest versions, but to have to rely on older generation technology for stability. Having clarified these aspects, the following part of the text will go into detail in describing the core principles of the proposed model.

The model structure can be summarized in the following way:

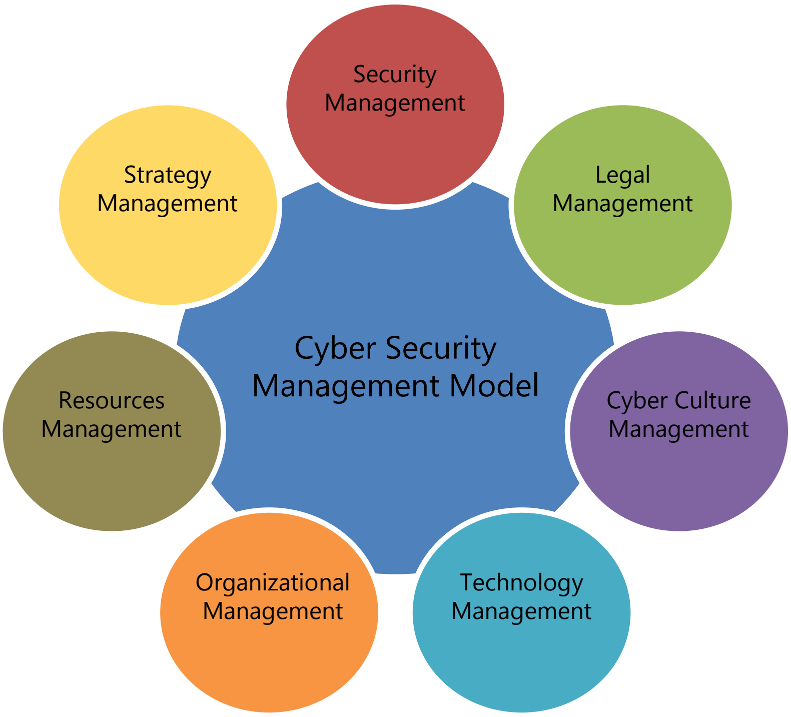


Figure 1. Cyber Security Management Model for Critical energy Infrastructures.
Source: made by the authors

As it is shown in Figure 1, the model consists of *seven* core categories applicable to every type of CEI, which are:

- *Resources Management:* the first category of the model, and probably the most important, describes the skeleton of the system to whom the model is applied.. Agencies need to know all of the elements, which are part of their physical system and to be aware of their vulnerabilities and weak links of their existing security systems (GEANT, 2019). This category should for this reason be one of the first to be considered in the implementation of the model since it is particularly useful in the preparation of the rest of the categories, but it is also useful for the process of monitoring the modifications to the system. This category aims to determine the state of security of the system, by assessing the physical security of the infrastructure and considering the physical assets of the CI, by determining the modalities of access control used in the facility, and finally the classification of the vulnerabilities of the establishment.

- *Organizational Management:* This category provides insights on the guidelines to be used in the direct response to cyber-attacks, which is of the utmost importance in emergencies. The focus on the category is mostly on the aftermath of the attack, namely the Disaster Recovery Planning, which comprehends the general instruction on how to behave in the various scenarios post-cyber-attack. Moreover, it offers a focus as well on Operational Security, which clarifies various techniques employable for the prevention and the response to cyber-attacks.

- *Technology Management* is another important category for the model, as it determines the cybersecurity of software, telecommunications, and network. While the Organizational category treated the physical security of the infrastructure, in this case, the focus is on the quality of the IT environment employed, with the implementation of various cybersecurity techniques, which will be varying according to the type of software and infrastructure the model is applied to.

- *Cyber Culture Management* category deals with the informational aspects of cybersecurity, as well as the "human" part of the system. It is the priority of this category to determine the safety of the employees as well as to raise awareness and training the staff to understand the basics of cybersecurity management.

- *Legal Management* is without a doubt an interesting addition to the model, as it gives the possibility of incorporating a pre-existing framework to the model: since the latter is qualified to apply to every type of CI, such category is needed to add to each model more characteristics that are specific and recommendations.

- *Security Management:* the aspects treated in this category are focused on cyber incident management, which means the guidelines to develop an effective management plan to be applicable in an emergency, and which covers every aspect of the event, from the preparation to the identification and handling, as well as the follow-up. The category will as well offer more information on the planning for other non-cyber-related consequences such as physical incidents and safety management.

- *Strategy Management* deals mainly with the techniques employed by the model in general, such as the calculations, as well as the detection of other present CEI that may be linked to the one to which the model is applied to.

In order to demonstrate the validity of the application of a management model for CEI, various pre-existent management models for cybersecurity will be analyzed and evaluate their efficiency in protecting CEI, especially considering the implementation of newer methods such as big data analysis used by such systems. The first framework that is taken into consideration for the analysis is the *COBIT 2019*, a framework developed for the governance and the management of IT, aimed at whole enterprises (ISACA, 2018). The further analysis considered as well the *NERC Implementation Guidance for CIP-008-6* (NERC, 2019), which aims to determine the incident response plan to cyber-based attacks in enterprises, as well as classification and prevention of damage from the management point of view. Another important framework that was taken into consideration is the *NIST Guidelines for Smart Grid Cybersecurity* (NIST, 2014, 2018), which serves as a national-level framework that can be applied to multiple sectors, and is a further evolution of Critical Infrastructure Protection (CIP). Another important management model that is taken into consideration is the *Cyber Security Management Model for Critical energy Infrastructure* developed by Limba et al. (2017), which is concerned with technological aspects used for CIP from cyber-based attacks and vulnerabilities. The analysis in the paper is presented in the following way: every mentioned document is presented with a short paragraph that considers the elements of such a framework that could be part of an adequate management model for CEIP. Rather than explaining extensively the contents of each document, the focus is on the parts that the authors considered being necessary to develop such a framework. Particular attention is made concerning the solutions to vulnerabilities linked to the aforementioned advanced techniques in CEIP such as AI or ML. The final step of the analysis will be the development of an additional series of criteria that might be integrated into the aforementioned framework for CEIP.

The main framework that was used in the analysis is the *COBIT 2019*, developed by ISACA as a framework that aims to develop and promote the process of understanding, designing, and implementing "*enterprise governance of IT" (EGIT)* (ISACA, 2018). The framework is periodically reviewed, as the one considered for this article is the one used in 2020, which was published in 2018. The framework offers an interesting take on the possible governance and management of IT aimed at enterprises, which can be applied in various branches of the latter. There are a few elements that are used by this framework that are particularly suitable for developing a management framework of CEI, although as mentioned before, this document offers a model that can manage various aspects of an enterprise (ISACA, 2018). It is important to mention that, at the beginning of the document, a differentiation is made between the concept of *governance* and *management*: the first is considered a responsibility of the board of directors, which then sets directions that are followed in *management* plans, which are considered responsibilities of the executive management under the CEO of the enterprise (ISACA, 2018). This offers valuable insight into the *responsibilities* within an enterprise and renders the response to emergencies much quicker.

Furtherly, the *COBIT Components of a Governance System* represents a useful tool for the classification, preparation, and management of an enterprise's core elements (ISACA, 2018). The criteria, which are used to characterize the *Governance System,* according to *COBIT,* are seven: a) *Processes, b) Organizational Structures, c) Services, Infrastructures, and Applications, d) Principles, Policies, Procedures, e) Culture, Ethics, and Behaviour* and *f) Information* (ISACA, 2018). The criteria which were found particularly useful for the purposed of the model are firstly *a) Processes,* which possess a rating system with whom are evaluated the capabilities level for each process: the range goes from 0, which represents the absence of any basic capability, to 5, which represents the full achievement of the process' purpose (ISACA, 2018). This aspect was taken as a possible system of classification of the enterprise's preexisting systems and elements, given that a complex classification usually is more adequate in case of emergencies, because an enterprise that knows all of its components knows as well all of its vulnerabilities. Another interesting category, which was taken into consideration, is *b) Organizational Structures:* the model offers a wide classification of various roles within the enterprise not only by defining their role in the company but by classifying them in a system that considers their different levels of *responsibility* (who drives the task?) and *accountability* (who accounts for the task's success?) (ISACA, 2018). A culture of security can be seen as *"behaviour and relations of individuals and employee teams, in courts and attitudes, in the way problems and conflicts are solved, work organization and human interaction"* (Gierszewski, 2020). As the aforementioned classification is considered as a way to improve the security of an enterprise, the development of a system clarifying *roles* and *responsibilities* would improve the quickness of response as well in terms of identifying the vulnerable elements of the system in case of cyber-based attacks (IEEE Standards 2013). Another important element of the *COBIT* model is represented by the category *d) Principles, Policies, Procedures:* the model proposed by ISACA reserves an additional category, which consists of adding to any process the possibility to reference a particular process or additional framework as a *third-party service,* by integrating it to the existent model. This solution is a great approach to consider in developing an effective model, given that these additional protocols or frameworks can change and evolve with time, and consequently modernize the "base" framework. These elements offered by the *COBIT* framework are fit for the model concerning CEIP; hence, they are taken into consideration for the final model.

Another important document that was considered for the analysis was the *NERC Implementation Guidance for CIP-008-6,* published by the North American Electric Reliability Corporation in 2018 (NERC, 2019). The document is mainly used, as it is said in the title, for the North American electricity systems, aiming in particular to CIP. The document offers useful insights for CIP and possesses an approach that is based on the response of cyber-based incidents or attacks in CI. An interesting element within the framework is the *Classification of Cyber Incidents:* as the classification of an enterprise's elements is useful for preventing a cyber-attack, a system that evaluates an enterprise's vulnerabilities can help in developing appropriate responses and solutions to various situations. The classification of cyber-incidents offered by the *NERC* system comprehends 6 levels, *Baseline (0), Low (1), Medium (2), High (3), Severe (4),* and *Emergency (5),* and is based on the attack's consequences (NERC, 2019). Besides, such classification provides as well a report ability threshold, by which only incidents with a level superior or equal to 3 are reportable to the responsible authorities: this prevents an overcharge of aid requests within an enterprise. Moreover, the other interesting element, which was found within the framework, is the role of the *E-ISAC/ NCCIC Reporting Coordinator,* which is responsible for the coordination of regulatory reporting activities related to E-ISAC (Electricity Information Sharing and Analysis Center) and the NCCIC regulatory framework (NERC 2019). The role of such authority within an enterprise is to determine the need to contact third-party services or international authorities in case of a severe cyber-attack and could be useful for the security of the enterprise. As it was reported in the article by Pl□ta et al. (2020) on cybersecurity management aspects, the NERC framework relies on the NIST guidelines; the introduction of the classification of Cyber Incidents based on a risk-assessment method could be a valid technique to develop in a general model (Pl□ta et al., 2020).

The *NIST Guidelines for Smart Grid Cybersecurity* is a sector-specific management framework dedicated to North American Smart Grid systems, developed by the National Institute of Standards and Technology (NIST) in 2014 (NIST, 2014). Although the model developed within the article is targeted to all types of CEI, this document provides an interesting take on key management techniques: smart grid systems possess more technology that is advanced in security systems, with the aforementioned implementation of big data analysis. Hence, the document offers a more up-to-date type of technology management solutions in terms of security requirements. The mentions in the document are a few and include the employment of *symmetric ciphers* for authentication and encryption, *public-key cryptography*, which needs to be supported by a hardware (cryptography co-processor) or in software (NIST, 2014). Additionally, the employment of *public-key certificates,* which are *"bind user or device names to a public key through some third-party attestation mode"* (NIST, 2014).

The model was originally developed specifically for CIP from cyber/based attacks, in particular relating to the security of Industrial Control Systems (ICS). The interesting aspect offered by the model is that it offers an insight into the development of the ICS in terms of protection: although ICS were considered part of the Operational Technology (OT) security, further digitalization of industrial technology brought the merging of Informational Technology (IT) and OT systems for ICSs. An issue highlighted by the authors is that, given the merging of OT and IT technology, it is needed for ICS to develop a security model that considers both environments, including a supply management system that can sustain cybersecurity aspects (Limba et al., 2017). Moreover, the model proposed by Limba et al. (2017) is particularly focused on the technology management aspects of cybersecurity, which is mentioned in one of the six categories developed, *technology management*: the text describes the latter as the understanding and classification of each component of the enterprise, and the consequent vulnerabilities (Limba et al., 2017). Considering this element, there could be an evolution of the category in terms of the effectiveness of each technique used for technology management, including big data analysis: hence, it can be useful for the analysis.

Given the previous overview of different pre-existing management models for CEI, this part of the article will be dedicated to the proposal of a management model for cybersecurity that can be used for all types of CEI. The ultimate aim of the model is to achieve an adequate level of cybersecurity. The aforementioned analysis provided useful insight on some elements, which were integrated into the model made by the authors. The elements, which are taken into consideration, are:

Processes, which can be described as the whole set of practices and activities, which altogether, achieve full cybersecurity. The general definition is taken from the one used in the COBIT 2019 protocol, which for each process appoints one or more activity (ISACA, 2018). The classification of such a process should include all the stages needed for the implementation of an adequate management strategy for implementing cybersecurity, covering the aspects of prevention, intervention, and recovery from a cyber-related threat. Moreover, to classify an enterprise's assets, each process will be assigned a value, which will reflect the level of implementation: the range will go from 0 to 5, in which 0 represents the total lack of implementation and 5 represents the full achievement of the process' purpose (ISACA, 2018). By using this solution, not only the development of a management strategy is easier, but also it is immediately noticeable what are a system's flaws and vulnerable points.

Roles and Responsibilities: as Stefaniuk (2020) puts it, "employees' improper conduct or lack of action lead to the majority of information security incidents" (Stefaniuk, 2020). Hence, this element is highly useful for the organizational aspects of management since the purpose of the latter is to determine and classify the roles within an enterprise, including a short description of the role's priorities. Moreover, this element will relate to the processes described in the previous paragraph, for the roles will each be given responsibility for one or more processes, to speed up the response in an emergency, and to determine the weak links of the systems in such situations. The development of such element should as well follow the directives offered by the COBIT 2019 framework, although it would be useful to develop a specific role for reporting cyber incidents, active at all times, to whom the members of the organization could turn to in the time of need, much like the role of the E-ISAC/NCCIC Reporting coordination mentioned in the NERC framework (NERC, 2019).

Technology management covers the more technical aspects of management: given that the model targets various types of CEI, this element will be more specifically dedicated to the classification of the technical components used for the enterprise's security, including the types of techniques. This also means that there will be a general classification of security technology techniques applicable to every CEI, and possibly the development of specific sections for CEI types. Moreover, the development of this element will as well have a focus on technical aspects and will offer a classification of the security techniques, which will be ranked in terms of effectiveness and innovation. In this way, a system will gain a higher mark if it possesses newer and effective security technology techniques, however still considering the aforementioned n-1 principle.

The Policy is one of the most innovative aspects of management modelling: as aforementioned, this model is applicable to every type of CEI, and for the model to be capable to do so, the more specific aspects of security management for every CEI are not mentioned right away. To resolve this issue and still propose an adequate and comprehensive model, there will be an additional category, which will include the implementation of other frameworks relative to the specific CEI to whom the model is applied to. Moreover, for each mentioned CEI there will be the possibility to integrate the model with countless other protocols, which could be substituted as newer versions are published, making the model suitable for long periods.

The last one is Vulnerabilities, which completes the organizational management aspects: along with processes and techniques employed within the enterprise, it is important as well to consider the possible weak points of the system by testing and classifying the vulnerabilities of the system. By doing this, not only it is easier to develop fast solutions preventively, but it is also a necessary step to not be caught unprepared in emergencies. The element could as well be improved by considering a ranking of vulnerabilities, which is based on the consequences of a potential cyber-attack, could have to the weak points of the system. In this case, it would be the management's job to determine the cases in which it is necessary to contact official authorities, hence speeding up the process of recovery in case of cyber-attack.

Critical energy infrastructures, especially European critical energy infrastructures, uses best practices, and methodologies to prevent, detect, identify and countermeasure effectively with cyber-attacks. It is a framework that has been designed by implementing it promotes the necessary measures and activates the necessary security mechanisms in order to avoid unpleasant situations. Cyber-attacks on critical energy infrastructures are not easy. Critical energy infrastructures are quite well protected, although technological advances have significantly upgraded their modes of operation while at the same time partially threatening them, in the past ICS operated in isolated environments, i.e. in isolated computer networks and used its own communications protocols and special software. The innovation of technology and networking has created quite a few cheap and, in some cases, undoubtedly quality devices that connect very easily to the network. Existing security equipment, security policies, and staff training do not currently allow critical energy infrastructures systems to be compromised to such extent as to affect their operation, nor to affect the goods they produce and store. Technological progress is rapid, new tools will be created to breach critical energy infrastructures systems, so critical energy infrastructures will need to immediately implement future risk forecasting models designed to shield their networks and systems in a timely manner, as will evolve and become more dangerous and larger in scale, if the upgrade of critical energy infrastructures systems is not followed then successful attacks will be preceded by the corresponding countermeasures [7].

The design and development of critical energy infrastructures information systems must take into account infrastructure security policy, operating parameters, requirements, support, and finally the smooth operation of software applications or the smooth transition of old software applications to new applications where work harmoniously with other software applications without creating incompatibility problems in some areas or processes. The security of information and industrial systems in critical energy infrastructures is an ongoing process, which cannot be ensured because of a single network product or a single information technology or information systems and infrastructure security. Needed a complete solution accompanied by the right security practices and methods to thrive on a comprehensive response to threats and attacks, practices and methods ranging from Firewalls, DMZs, to forecasting models and attack detection mechanisms before they grow.

PART II: HOW TO CREATE SOC (PREPARATION)

How to create a security operations center (SOC) - preparation

Cybersecurity threats are becoming more manifold. Therefore, at this moment it is difficult to say that the critical energy infrastructure is compromised or not. Afterall according to the statistics, the average number of days from the initial breach to detection is from 210 days to 254 days (Trustwave, 2014). Critical energy infrastructure must have the ability to detect and respond the security incidents. However, data security needs increase over time until a dedicated Security Operations Center (SOC) is required, which is the foundation of incident management process. However, before looking at the basic steps for setting up an SOC, it is worth asking the question: how can you improve your security incident management capabilities without investing a lot of money? The answer lies in understanding the current capabilities of people, processes and technologies.

Not everyone needs their own incident response team. This need must be assessed against a number of factors, including budget. Therefore, it is necessary to evaluate all the factors that influence whether a custom SOC is needed. There is no standard guidance for knowing whether or not to set up your own SOC. Therefore, you can start by answering a questionnaire (see Annex II) that will help determine if a given support group can support SOC or if the group should receive services from an external organization.

The SOC is a specialized IT department that monitors, detects, investigates and responds to multiple types of cyber threats, protecting enterprise networks, equipment, software, websites from security intrusions. The SOC continually scans the network for threats, weaknesses, and deficiencies to mitigate before they turn into critical issues or incidents. SOC cyber security operations incorporate tools and processes such as security information and event management systems (SIEMs), breach and instruction detection, firewalls, and probes. SOC monitoring and investigation activities focus on daily operational security and are less concerned with designing or developing security strategies and architecture (Figure. 2). [14].

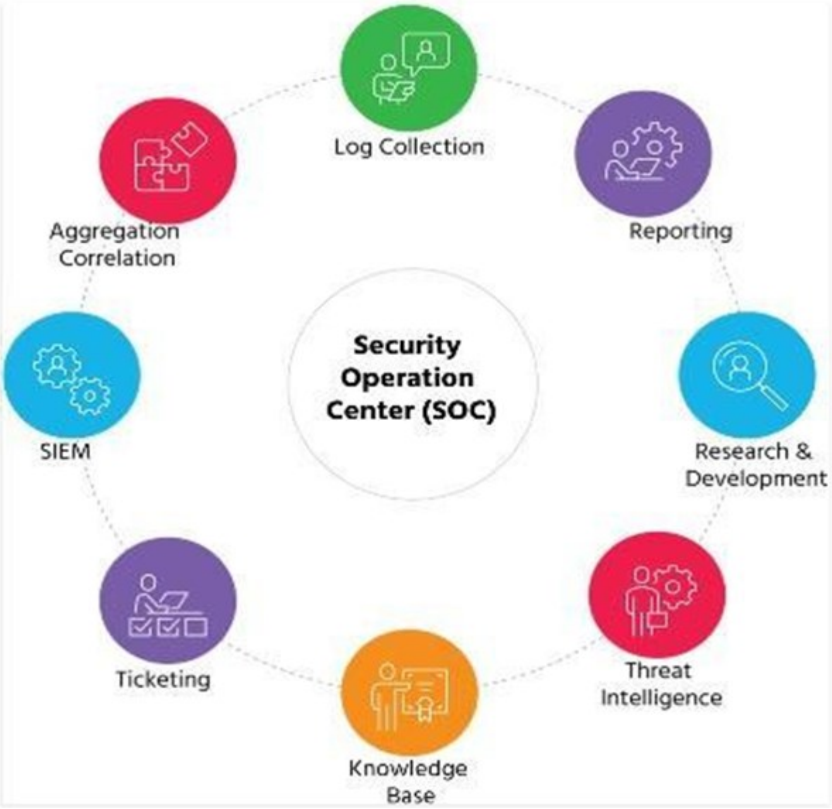


Figure 2. SOCs use multiple processes and tools to reduce or negate security threats. (Source: Mark Roy Long)

Step 1: Legal Management

In order to properly plan, design the SOC and control costs, it is necessary to carefully plan everything, considering of the following elements:

1. Risk assessment:

Would-be attackers or even third country governments trying to strike at third countries to manipulate them and diminish their image of international trust, easily target critical energy infrastructures because of the importance of their operation and the key roles they play. Critical energy infrastructures are often inspected for proper compliance with security methods and protection of the infrastructure from cyber-attacks. Checks for vulnerabilities in applications and malfunctions of industrial systems must be thorough. That why first at all must perform risk assessments to identify priorities. Risk Analysis is a very important entity, the reason is that a risk assessment is performed, which assessment identifies the security problems that exist in relation to the possible damages that may be caused.

Risks must be assessed and the level of each risk assessed before the actual event occurs, depending on the critical energy infrastructures both the response and emergency plan and the category of equipment to be used vary. Risk Analysis helps identify the likelihood that a threat will materialize in conjunction with the impact that this threat will have in industrial systems through cost analysis. The key to success is the right foundations from the beginning of the process such as the correct and expanded collection of information, the correct analysis of the collected information, the clear definition of objectives, the analysis and evaluation of available resources, the inability to implement a strategy or due to unavailable resources or non-compliance with security policy.

Critical energy infrastructures protection measures should include the design of an integrated risk and impact management model, a prerequisite for the management model design is the safety policy analysis and risk management. Priority definitions and risk priority assessments that include sensitive vulnerabilities, general weaknesses, security vulnerabilities, including staff, should be assessed and the risk of hazards impact which will help a lot in terms of developing the framework design, the proper allocation of resources, responsibilities, and the creation of specialized protection measures.

Absolute security is nowhere to be found, which is why ongoing studies and future prediction studies tend to predict future attack methods to shield information systems against these new threats. This is something that comes with constantly updating the security policy. Critical energy infrastructures need to update their studies on the security of their information systems and networks, including their industrial equipment, which is why risk and needs analysis are two interrelated entities. Another important entity is the impact assessment analysis including the impact on infrastructure resources, such as calculating available resources and if these available resources can be utilized in different ways to limit an impending attack on the future, they must also to create studies regarding the level of impact within the infrastructure and to what extent they are able to influence the operation of the infrastructure, the production or to reduce its productive capacity and how this can be reduced.

Critical energy infrastructures operate based on the legal framework of the country in which they are based and always in accordance with the European framework of operation and of course always follow their security policy, which is always in line with the national security policy of critical energy infrastructures.

The planning of security policy as well as its application should be done by dividing roles and actions in order to be effective and to work at the right time based on the action plan and not individual actions. A critical energy infrastructures security policy includes a description of goals, key principles, objectives, and future objectives. It is an official form, which the administration and the staff should be respected and observed with reverence. The security policy defines and describes the duties of the personnel in managing security issues and defining actions such as communication with other sectors, implementation of appropriate procedures, control and management, system administration, etc. Of course, a security policy not only describes the responsibilities and functions, but also defines the responsibilities of the managers and specialized executives of an infrastructure.

The implemented critical energy infrastructures security policy should evaluate each sector as an entity, which means that the evaluation should not be uniform for all, it should take into account the criticality of each sector, it should implement the layout policy of the 6 sectors according to their criticality, as described below.

Sector 1: Security of the perimeter of a critical energy infrastructure.
Sector 2: Indoor / Outdoor Entries.
Sector 3: Shared areas within the critical energy infrastructures.
Sector 4: Office Areas.
Sector 5: Critical Industrial Sector / systems control.
Sector 6: Very Critical Industrial Sector / Systems Control.

The implementation of security sectors in a security policy is very important because each sector has different security requirements, and in addition, there is the possibility of implementing strong security policies between the sectors, especially the critical and very critical sectors. Should not overlooked the fact that critical energy infrastructures are very expensive and choosing the cost of a damage would be huge because those parts that have been damaged will have to be repaired or replaced, in addition the social cost is huge as services to citizens will not be can be provided such as energy or fuel.

2. Business case:

After analyzing the risks, it is necessary to establish the goals and objectives that the critical energy infrastructure sets for itself. Also, do not forget about the business case, paying attention to short and long-term investments. Goals, objectives, technical and other requirements for the system, necessary investment must be documented. Therefore, it is necessary to create a business case that will combine all of the above, including the section on staff qualification requirements. This section could include details such as; what is the staff skills required to run a SOC and, what are the current skills, and what training is required (*Global Information Assurance Certification Paper*).

Creating a business case for an SOC system, do not complicate things. It is necessary to start simple and gradually move to more complex things, because for many the SOCs system is a new thing. Therefore, the SOC strategy should consist of the following aspects, which will be agreed and documented (Figure 3):

- SOC mission
- SOC strategic goals
- SOC functional requirements
- SOC technical requirements
- SOC staff requirements
- SOC budget (investments)

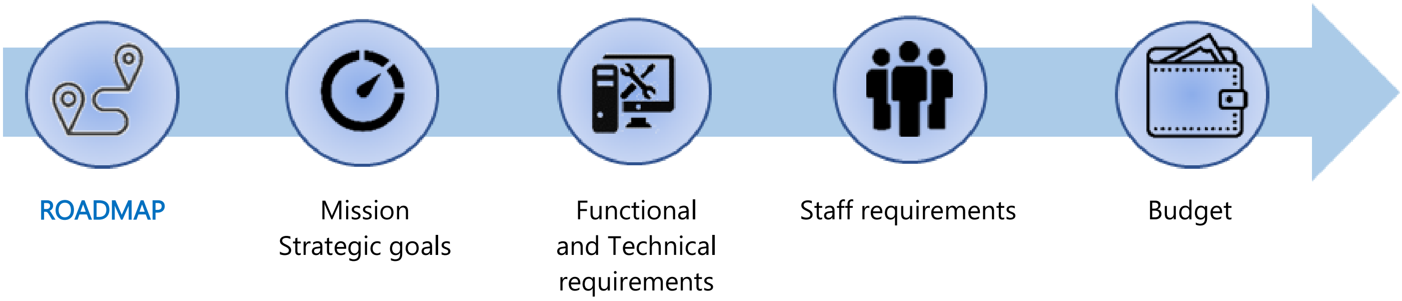


Figure 3. SOC roadmap. Source: author

Each element of the strategy will be described in detail in this book. To begin with, it is necessary to determine what elements should be included in the description of the mission of the SOC system. Based on MITER data, a typical midsize SOC's mission statement typically includes the following elements [15]:

- Preventing cybersecurity incidents through proactive measures, including:
  - Continuous analysis of threats
  - Scanning for vulnerabilities
  - Deploying coordinated countermeasures
  - Consulting on security policy and architecture

- Monitoring, detection, and analysis of potential intrusions in real time and through adversary hunting, utilizing a variety of security-relevant data sources

- Responding to confirmed incidents, by coordinating resources and directing use of timely and appropriate countermeasures

- Providing situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behavior to appropriate organizations

- Engineering and operating SOC technologies, such as host sensors, network sensors, log collection, and analysis systems.

In addition, the mission of the SOC can be viewed in terms of the infrastructure and data it protects. For the majority of SOCs, their responsibilities will also include monitoring, detecting, and responding to potential incidents on remote systems, systems and data in the cloud, and the constituency's mobile infrastructure [15]. The SOC is expected to be responsible for all of these aspects: IT (local and remote), OT, cloud and mobile.

Let's consider some SOC scoping examples from two industries [16].

Example 1: A Military Organization [16].

Mission Statement

The SOC monitors the overall security posture of all networks operated by the organization, including general and tactical networks. The SOC reacts to information security incidents with the objective of maintaining the overall security of the organization, supporting the readiness of the organization's offensive and defensive capabilities.

SOC Scope Statement

The SOC scope covers all locations across the country hosting systems owned and managed by all units that are connected to the general and tactical networks. The services offered by SOC include around-the-clock security monitoring of systems, applications, and networks with the objectives of detecting and reacting to all external attacks and insider malicious behaviors. The services offered by SOC are handling incident response; collecting and correlating the various system events from the various networks; capturing, analyzing, and storing raw packet data from all the security enclaves; discovering, assessing, and tracking vulnerabilities; and consuming any threat intelligence information received from other alliance military forces.

Example 2: A Financial Organization [16].

Mission Statement

The SOC monitors the security posture of networks, systems, and applications operated by IT, with the objective of detecting and reacting to information security incidents that could negatively affect the organization's business operation.

SOC Scope Statement

The SOC scope covers all systems that are managed and operated by IT, including these located in national and international offices. The SOC services are offered around the clock and include the collection and correlation of security events messages, handling distributed denial-of service attack, detecting internal and external malicious activities, responding to information security incidents, leading the computer security incident response team, and conducting awareness sessions when required.

SOC Model of Operation

One important decision that the SOC architecture team needs to consider during the planning phase is whether to internally develop SOC capabilities, outsource capabilities, or leverage a hybrid of these two approaches. This decision should be based on a number of factors, including the following:

- Cost of internally developing, operating, and maintaining acceptable levels of SOC capabilities versus outsourcing them. This should include whether outsourcing costs can be spread over a period of time versus the upfront costs of developing an in-house SOC.
- The availability of a reliable SOC service provider that can meet or exceed your service level agreements (SLA).
- Available resources and weighing value of outsourcing versus the cost to maintain internally.
- Regulations that might prohibit outsourcing all or some of the SOC services.
- Time required for creating in-house SOC documentation and processes.

Considering the technical requirements of the equipment, one should not forget about the processes that the SOC system would perform. Therefore, this guide proposes one of the methods for developing a system life cycle.

The System Development Life Cycle method is the oldest method of creating computer information systems that are to be used in large and complex infrastructure such as critical energy infrastructures. This methodology assumes that an information system has a predetermined lifespan, thus comparing it to the human life cycle that is to a living organism, classifying it into three categories, the beginning, the middle and the end, like in the case with humans, birth and growth, middle age, and death. The use of the System Development Life Cycle method consists of 6 stages, which are:

1. *Collection of information regarding the project who is under development.*
2. *Analysis of the information collected.*
3. *Design of the new system taking into account prerequisites and safety requirements.*
4. *Development of the information system.*
5. *Installation of the information system in the infrastructure.*
6. *Customization and user training.*

The implementation of each of the above stages presupposes the completion of specific tasks which after their completion the software implementation process is transferred to the next stage. Systems analysts and developers are responsible for most of the implementation of the new system, as the new system must be properly designed and implemented without security vulnerabilities, taking into account the security and information integrity specifications that it is going to manage. Analysts design the new system according to what information they have gathered by visiting critical energy infrastructures, talking to executives, and experienced staff using data gathering methods such as questionnaires or in-person interviews, while taking into account security policy which the new information system should be fully harmonized both for the security of the other infrastructure systems and for the proper operation of the new system. At the end of each stage, they evaluate in detail if all the safety and implementation requirements of the new system have been met, if all the conditions have been met then the implementation process goes to the next stage. Before starting the process of designing and implementing a new system, critical energy infrastructures managers should be able to answer the questions "why do we need this new system?", "With the development of the new system, what are the goals that will improve the current situation? ","is the new system who is under development able to improve important infrastructure functions? ", the above are some of the antenna questions that need to be answered before developing a new information system. If the critical energy infrastructures executives are able to answer qualitatively the above questions, then, the new information system is necessary for the critical energy infrastructures, and in the next step the general objectives of the new information system who is under development are identified, described in detail its objectives, the objectives of the project are described, and finally a project management plan is developed regarding the due date of its implementation. Critical energy infrastructures managers, once informed, can make their proposals regarding security issues, security policies that should be taken into account, and anything else that is inconsistent with the secure operation of the information system of the infrastructure.

The System Development Life Cycle method, as mentioned above, is widely used to create information systems that address large infrastructure, including critical energy infrastructures. Critical energy infrastructures need a thorough analysis of both the requirements and the security specifications; they need strict process controls during the process of developing information systems.

The management and implementation of safety practices in critical energy infrastructures is a business process. Its purpose is to identify security vulnerabilities, assess them based on a risk scale, and then make the appropriate decisions in order for the infrastructure to patch the security vulnerabilities immediately. Actions must be coordinated as well as procedures in order to be effective, action results must be re-evaluated to check their effectiveness. It is a process that will be carried out regularly as the requirements for security and accuracy of information and the security of control mechanisms are constantly growing. There are some steps may take to begin the process of preparation for mediation.

1. *Infrastructure and management staff are required to carry out security checks on the infrastructure.*
2. *Determination of the size and extent of the examination of the systems.*
3. *Determining the safety vulnerabilities and using a risk assessment measure.*
4. *Evaluation of findings and evaluation of security requirements.*
5. *Check for security vulnerabilities that have been identified and addressed by implementing the security policy.*

An important role in the effectiveness of security as well as in the methods of incidence response to cyber-attacks is the cost of implementing both security measures and countermeasures. The limited cost of implementing incident response systems and practices creates complex or incomplete methods that are either insufficient or, due to their complexity, not fully understood by staff. The cost of implementing a security policy must be assessed on the one hand taking into account the security of infrastructure systems and on the other hand the cost of damage and repair.

3. SOC process:

SOC can perform more than 40 main functions: from collecting data on incidents to interacting with law enforcement agencies, from analyzing malicious code to raising employee awareness. It is worth noting that basically there are no such SOC systems that successfully perform all these functions simultaneously. Probably, such systems do not exist at all. Therefore, it is necessary to choose the main functions that your system will perform. The Table 1 shows all the func-

Incident Triage, Analysis, and Response	
Real-Time Alert Monitoring and Triage	Performing triage and short-turn analysis of potential security incidents generated by near- real-time security alert feeds.
Incident Reporting Acceptance	Receiving and processing reports of potential security incidents from constituents, other SOCs, and third parties. These reports may come through written (e.g., email) or verbal means.
Incident Analysis and Investigation	Performing in-depth, detailed analysis of suspected incidents. This includes identifying details such as the origin, extent, and implications of an incident, and characterizing the confidence of these conclusions.
Containment, Eradication, and Recovery	Performing activities supporting incident/adversary containment, damage management, adversary eviction, and system recovery to reduce current impact and move to a state that will prevent future incidents.
Incident Coordination	Performing information gathering, information distribution, and notification in support of an ongoing incident. Directing and/or coordinating response in partnership with constituents, incident response stakeholders, other SOCs, and third parties.
Forensic Artifact Analysis	Examining media samples and digital artifacts (hard drives, files, memory) to draw detailed observations and conclusions about suspected activity, such as content analysis and timeline reconstruction.
Malware Analysis	Examining suspicious files to understand the provenance, pedigree, functions, and intent of suspected malware samples. This includes utilizing various methodologies, including static code reverse engineering and dynamic runtime analysis.
Fly-Away Incident Response	Tools, procedures, and coordination practiced to rapidly relocate and provide onsite incident response services for constituents at physical locations where SOC analysts do not routinely reside.
Cyber Threat Intelligence, Hunting, and Analytics	
Cyber Threat Intelligence Collection, Processing, and Fusion	Collecting cyber threat intelligence products, including CTI feeds and reports. Processing and integrating CTI into SOC systems and parsing and filtering information for further consumption by the SOC and its constituency.
Cyber Threat Intelligence Analysis and Production	Utilizing analytic techniques to track, trend, and correlate adversary behavior over time, and support risk decision making. This includes creating and producing CTI reports describing specific adversaries, their TTPs, and campaigns. This may include using a cyber threat intelligence platform or other tools to enhance analysis.
Cyber Threat Intelligence Sharing and Distribution	Sharing CTI and incident reports with parties outside the SOC, including partners, other SOCs, and the broader cybersecurity community.

Threat Hunting	Performing proactive operations to identify potentially malicious activity, outside the scope of established SOC alerts, based on hypotheses that the adversary is operating in or against the constituency. This includes developing and refining custom analytic capabilities.
Sensor and Analytics Tuning	Performing curation, tuning and optimization of detections, analytics, signatures, correlation rules, and response rules deployed on SOC detection and analytics systems, such as EDR, SEIM, and SOAR.
Custom Analytics and Detection Creation	Using knowledge of adversary TTPs and constituency systems to create detections and analytics to detect and understand various activity in SOC sensors and analytic systems, usually from scratch.
Data Science and Machine Learning	Defining, implementing, and curating data science and machine learning techniques to support SOC functions, such as bespoke machine learning models tailored to the constituency.
Expanded SOC Operations	
Attack Simulation and Assessments	Performing red teaming, pen testing, adversary emulation, purple teaming, breach and attack simulation, or other testing detections with the goal of improving SOC operations and the constituency's overall defensive posture.
Deception	Performing actions to conceal networks and assets, create uncertainty and confusion, and/or influence and misdirect adversary perceptions and decisions.
Insider Threat	Supporting detections, analytics, and investigations focused on finding malicious or anomalous activities carried out by users with legitimate access to constituency systems.
Vulnerability Management	
Asset Mapping and Composite Inventory	Collecting and curating knowledge of constituency assets, networks, and services, mapping their interdependencies, and calculating criticality and risk.
Vulnerability Scanning	Interrogation of constituency assets for vulnerability status, including patch level and installed software, and security-relevant configuration, for purposes of calculating security risk and compliance status.
Vulnerability Assessment	Performing the "systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation." [11]
Vulnerability Report Intake and Analysis	Accepting, triaging, and analyzing vulnerability reports from vulnerability researchers to understand them and find mitigations for constituency products or assets. This is sometimes known as a responsible vulnerability disclosure program.
Vulnerability Research, Discovery, and Disclosure	Performing proactive discovery of security vulnerabilities not previously known to the SOC (e.g., "0 days"), through reviewing internal incidents, cyber threat intelligence collection, and software reverse engineering. This includes sharing vulnerability information with vendors, other SOCs, and constituents such that they can act on that information.
Vulnerability Patching and Mitigation	Addressing vulnerabilities through applying patches or mitigating the risk of vulnerability exploitation through minimizing vulnerability exposure to adversaries such as system or service configuration changes.
SOC Tools, Architecture, and Engineering	
Sensing and SOC Enclave Architecture	Defining the overall architecture for the sensing, analytic and SOC operating environments, including the integration between various components and data management planning. This may include evaluating commercial products for intended use.

Network Security Capability Engineering and Management	Engineering, deploying, operating, and maintaining network and enterprise services detection and protection capabilities including firewalls, web proxies, email proxies, and content filters. This includes creating and maintaining the connections and data flows that interconnect tools and data.
Endpoint Security Capability Engineering and Management	Engineering, deploying, operating, and maintaining endpoint detection and protection capabilities such as EDR. This includes creating and maintaining the connections and data flows that interconnect tools and data.
Cloud Security Capability Engineering and Management	Engineering, deploying, operating, and maintaining cloud detection and protections capabilities such as CASB and other cloud-native tools that protect cloud services. This includes creating and maintaining the connections and data flows that interconnect tools and data.
Mobile Security Capability Engineering and Management	Engineering, deploying, operating, and maintaining enterprise and endpoint detection and protection capabilities for mobile devices. This includes creating and maintaining the connections and data flows that interconnect tools and data.
Operational Technology Security Capability Engineering and Management	Engineering, deploying, operating, and maintaining cyber detection and protection capabilities for operational technologies. This includes creating and maintaining the connections and data flows that interconnect tools and data.
Analytic Platform Engineering and Management	Engineering, deploying, operating, and maintaining SIEM, SOAR, CTI platforms, UEBA, Big Data Platform, and other technologies. This includes creating and maintaining the connections and data flows that interconnect tools and data.
SOC Enclave Engineering and Management	Deploying, operating, and maintaining technologies, outside the scope of SOC and sensor capabilities, that support SOC operations including research environments, servers, workstations, printers, file shares, and enclave network systems.
Custom Capability Development	Creating the custom tools and systems necessary to fulfill various SOC requirements when no suitable commercial or open-source capability fits the need.
Situational Awareness, Communications, and Training	
Situational Awareness and Communications	Synthesizing and redistributing the SOC's knowledge of constituency assets, risks, threats, incidents, and vulnerabilities to constituents, supporting improvement of constituency cybersecurity posture and practices. Engaging within the constituency, and with other external organizations, to inform and be informed, collaborate, and share information.
Internal Training and Education	Gathering, formulating, and delivering training to SOC analysts to increase their proficiency in SOC functional areas.
External Training and Education	Gathering, formulating, and delivering training to constituents, to increase their knowledge of various cybersecurity topics.
Exercises	Formulating and facilitating cybersecurity scenario-based simulations and exercises, such as mock critical severity incidents.
Leadership and Management	
SOC Operations Management	Executing the day-to-day functions of running a SOC including financial and personnel management.
Strategy, Planning, and Process Improvement	Identifying the future state of the SOC and guiding the organization towards those outcomes. This includes looking at and learning from the past, performing assessments of the current state, and identifying new opportunities.
Continuity of Operations	Creating and evaluating plans designed to help the SOC sustain mission and business processes during and after a disruption.
Metrics	Defining, measuring, and reporting on key performance indicators of operational processes, the output of operations, and/or situational awareness of the constituency.

Table 1. SOC Function Categories and Function Areas.
Source: Kathryn Knerler, Ingrid Parker, Carson Zimmerman

At the beginning of SOC system construction, the “less but better” rule applies. It is worth concentrating on the key tasks facing the system being created, and describe the processes that ensure their implementation. At a minimum, it is necessary to collect, store and process data from information security and IT systems, enable users to report suspicious activity, investigate and respond to incidents. The SOC team needs to have up-to-date information about the infrastructure it protects and effectively interact with colleagues from other departments: IT and information security services, HR, lawyers, system owners, etc. Without this, it is difficult to imagine the work of the SOC; therefore, it is from this worth starting.

SOC processes and procedures can be depicted as a sequence of activities grouped by area of activity (Figure 4).

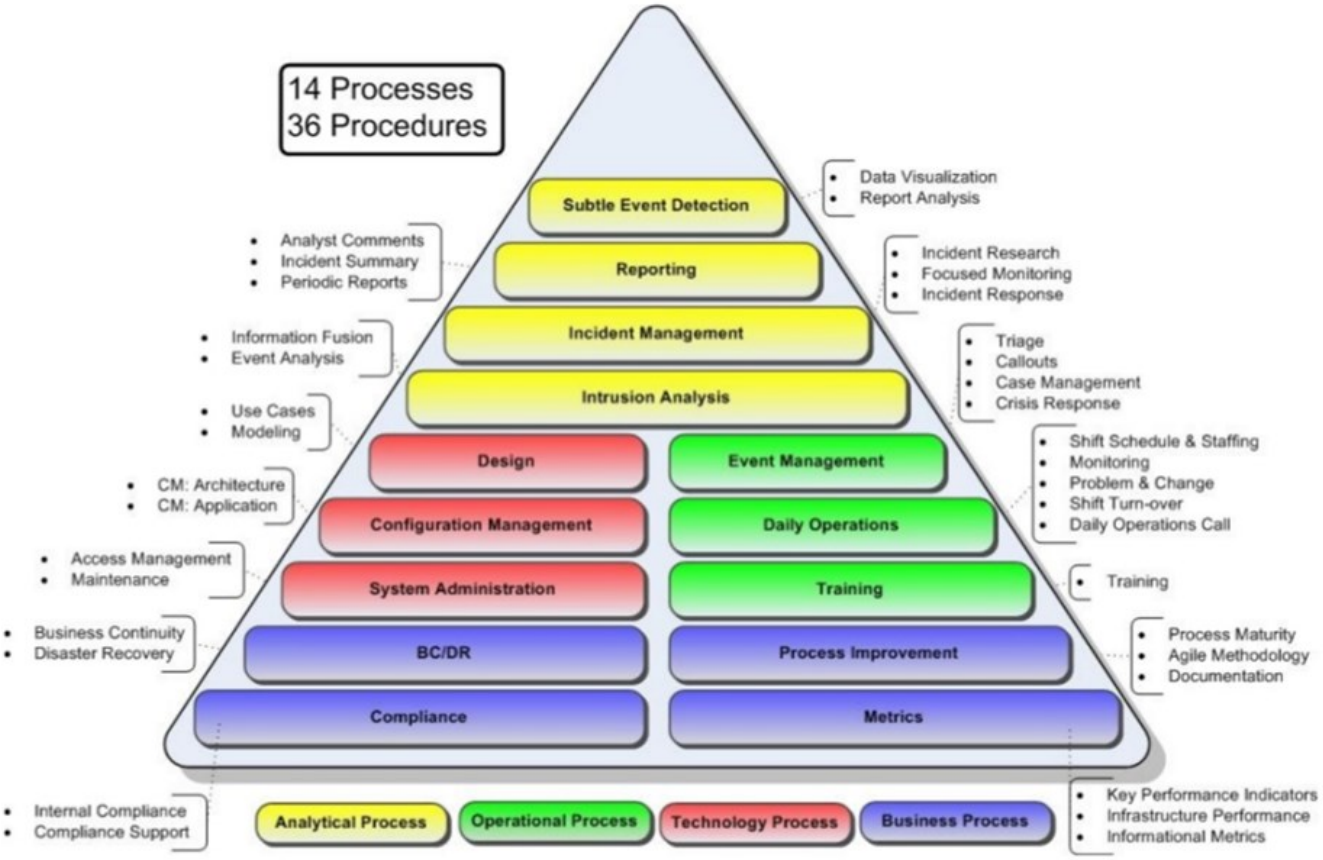


Figure 4. SOC processes and procedures.
Source: Hewlett-Packard Development Company

Despite the huge list of functions that the SOC system can perform, each organization focuses on its goals and objectives, on the available staff, and of course, the budget. Therefore, when drawing up a strategy, it is worth paying attention to the 10 main functions that any SOC system should perform [20]:

1. Take Stock of Available Resources

The SOC is responsible for two types of assets—the various devices, processes and applications they are charged with safeguarding, and the defensive tools at their disposal to help ensure this protection.

- **What The SOC Protects**

  The SOC cannot safeguard devices and data they cannot see. Without visibility and control from device to the cloud, there are likely to be blind spots in the network security posture that can be found and exploited. So, the SOC's goal is to gain a complete view of the business' threat landscape, including not only the various types of endpoints, servers and software on premises, but also third-party services and traffic flowing between these assets.
- **How The SOC Protects**

  The SOC should also have a complete understanding of all cybersecurity tools on hand and all workflows in use within the SOC. This increases agility and allows the SOC to run at peak efficiency.

2. Preparation and Preventative Maintenance

Even the most well-equipped and agile response processes are no match for preventing problems from occurring in the first place. To help keep attackers at bay, the SOC implements preventative measures, which can be divided into two main categories.

- **Preparation**

  Team members should stay informed on the newest security innovations, the latest trends in cybercrime and the development of new threats on the horizon. This research can help inform the creation a security roadmap that will provide direction for the company's cybersecurity efforts going forward, and a disaster recovery plan that will serve as ready guidance in a worst-case scenario.
- **Preventative Maintenance**

  This step includes all actions taken to make successful attacks more difficult, including regularly maintaining and updating existing systems; updating firewall policies; patching vulnerabilities; and whitelisting, blacklisting and securing applications.

3. Continuous Proactive Monitoring

Tools used by the SOC scan the network 24/7 to flag any abnormalities or suspicious activities. Monitoring the network around the clock allows the SOC to be notified immediately of emerging threats, giving them the best chance to prevent or mitigate harm. Monitoring tools can include a **SIEM** or an EDR, better even a **SOAR** or an XDR, the most advanced of which can use behavioral analysis to "teach" systems the difference between regular day-to-day operations and actual threat behavior, minimizing the amount of triage and analysis that must be done by humans.

4. Alert Ranking and Management

When monitoring tools issue alerts, it is the responsibility of the SOC to look closely at each one, discard any false positives, and determine how aggressive any actual threats are and what they could be targeting. This allows them to triage emerging threats appropriately, handling the most urgent issues first.

5. Threat Response

Most people think of when they think of the SOC. these actions As soon as an incident is confirmed, the SOC acts as first responder, performing actions like shutting down or isolating endpoints, terminating harmful processes (or preventing them from executing), deleting files, and more. The goal is to respond to the extent necessary while having as small an impact on business continuity as possible.

6. Recovery and Remediation

In the aftermath of an incident, the SOC will work to restore systems and recover any lost or compromised data. This may include wiping and restarting endpoints, reconfiguring systems or, in the case of ransomware attacks, deploying viable backups in order to circumvent the ransomware. When successful, this step will return the network to the state it was in prior to the incident.

7. Log Management

The SOC is responsible for collecting, maintaining, and regularly reviewing the log of all network activity and communications for the entire organization. This data helps define a baseline for “normal” network activity, can reveal the existence of threats, and can be used for remediation and forensics in the aftermath of an incident. Many SOCs use a SIEM to aggregate and correlate the data feeds from applications, firewalls, operating systems and endpoints, all of which produce their own internal logs.

8. Root Cause Investigation

In the aftermath of an incident, the SOC is responsible for figuring out exactly what happened when, how and why. During this investigation, the SOC uses log data and other information to trace the problem to its source, which will help them prevent similar problems from occurring in the future.

9. Security Refinement and Improvement

Cybercriminals are constantly refining their tools and tactics—and in order to stay ahead of them, the SOC needs to implement improvements on a continuous basis. During this step, the plans outlined in the Security Road Map come to life, but this refinement can also include hands-on practices such as red teaming and purple teaming.

10. Compliance Management

Many of the SOC’s processes are guided by established best practices, but some are governed by compliance requirements. The SOC is responsible for regularly auditing their systems to ensure compliance with such regulations, which may be issued by their organization, by their industry, or by governing bodies. Examples of these regulations include GDPR, HIPAA, and PCI DSS. Acting in accordance with these regulations not only helps safeguard the sensitive data that the company has been entrusted with—it can also shield the organization from reputational damage and legal challenges resulting from a breach.

Whatever processes and procedures the SOC system would follow, they must be recorded on paper. All organizations have adopted a different level of documentation, but at least in a minimal form at this stage it should be so that all participants in the process (and there are many of them) build the same thing.

Only now, having an idea of what exactly needs to be automated, can we proceed to the choice of technical means. In addition to the traditional SIEM system, you will need many additional tools, often inexpensive or free, but requiring certain knowledge from the SOC staff. The very requirements for the "quality and quantity" of employees will also begin to emerge.

4. Current capabilities:

As already noted, SOC is primarily a team, and technical means are just a tool that will work only in capable hands. In the matter of recruiting personnel for the SOC under construction, it is worth proceeding from the principle "quality is more important than quantity". The main task is to ensure that top-level professionals are in key positions. This is the case when it is better to hire one "star" than two ordinary analysts (especially at the beginning of the creation of the SOC).

A strong team is critical to the success of any security operations center (SOC). As the front line for most security incident investigations and responses, they are expected to deliver a consistently robust set of services, often under great pressure and constraint. Individuals within such teams often require a wide range of technical and nontechnical skills, in addition to the ability to work effectively as a cohesive unit. In some SOCs, this also means a seamless stitching of many organizations, both internal and external, to deliver on the SOC's core mission [16]. So, perform a comprehensive audit to identify and leverage current capabilities to reduce costs and avoid redundancies [14].

Identifying gaps between the current and required skillset of the existing support staff should be the next step in formalizing a virtual SOC team. Formalize a training road map for each SOC team member based on the gap assessment results and then secure funds to execute train-

Team Member	Current Skills	Required Skills
Network Support Team member 1	Firewall administration Firewall Log analysis VPN (Virtual Private Network) & Access control Routing & Switching concepts TCP/IP concepts	Incident triage – Yr1 TCP/IP packet analysis (GCIA) – Yr2 Basic ethical hacking skills – Yr2 CISSP contents – Yr1 SIEM training – Yr1
Network Support Team number 2	IDS administration Configure and fine tune IDS TCP/IP packet analysis TCP/IP concepts	Incident Handling (GCIH) – Yr2 OS security concepts – Yr1 SIEM training – Yr1 Malware Analysis (GIAC Certified Reverse Engineering Malware – GREM) – Yr2
Operating System Team member 1	Win Server OS administration Anti-virus, Proxy & mail gateway	SIEM training – Yr1 GCIH training – Yr2 CISSP contents – Yr1 Incident triage – Yr1
Operating System Team member 2	Linux Server OS administration Mail server administration	TCP/IP packet analysis – Yr1 CISSP contents – Yr1 Incident triage – Yr1 Network security concepts – Yr1

SCADA Support Team member 1	Skillset 1 Skillset 2 Skillset3	Skillset 1 Skillset 2 Skillset3
SCADA Support Team member 2	Skillset 1 Skillset 2	Skillset 1 Skillset 2

Table 2. Training roadmap. Source: Babu Veerappa Srinivas

The SOC's strength comes from its narrow focus on security threats. While you may have current staff who can perform some SOC duties, invest in outside talent when necessary to create the best team [14].

Essential SOC personnel include [14]:

- **SOC manager:** Supervises the SOC team and reports to the chief information security officer (CISO)
- **Security analyst:** Provides real-time risk management and security intelligence
- **SIEM engineer:** Oversees SIEM administration, incident response, and vendor management
- **Forensic investigator:** Analyzes incident data, evidence, and behavior analytics
- **Incident responder:** Conducts initial investigations and threat assessments using incident response plans (IRPs)
- **Compliance auditor:** Ensures SOC procedures remain in compliance with government regulations and industry standards

A co-managed SOC, which combines internal employees with independent contractors, can reduce personnel overhead [14]. It is also necessary to send employees for training on the technical means used in the SOC. Such training will not make them experts, but it will allow them to quickly navigate complex products, such as SIEM or a security scanner. Training can be provided by an integrator or consultants involved in the implementation of the system. Such training includes not only technical points, but also procedures that are individual for a particular SOC. All new employees of the SOC must be trained to familiarize them with the duties, regulations and techniques. Otherwise, there is a risk of one day discovering that, for example, the first line has been missing critical incidents for 6 months. The collection and dissemination within the team of information about new threats and trends in information security should not be episodic events, but a well-functioning continuous process. An important component of training is the exchange of experience within the team, including within the framework of internal rotations.

Therefore, there was an understanding of what processes need to be automated so that the SOC department is not bogged down in routine work, sorting out all the incidents manually.

Most utilities have a Network Operation Centre (NOC) to monitor the IT network. SOC and NOC exhibit many similarities in their functioning but only the context is different. The context specific skills can be built by additional training for the existing staff. Staff experienced in servers, desktop and network support will have good troubleshooting skills, which are important skills required for SOC functionality and managing and investigating SIEM alerts. Additionally, they will have TCP/IP protocol suite knowledge and basic malware infection and propagation methods. Basic security training and certification, such as Certified Information Systems Security Professional (CISSP) and GIAC Certified Security Essentials (GIAC-GSEC), must compliment these skills. It is important to hire staff members based on the core requirements, historical knowledge of the organization, analytical mindset, process focused, attention to detail and good attitude. This recommendation is in line with the statement "bet on a great team rather than on a champion" by Yves Breta (Breta, Y. 2013). [17]

Based on the knowledge and qualifications of the technical staff, it is necessary to determine the technical requirements for the equipment that will be used in the SOC system. Some of the tools can be basic tools like antivirus, firewall and intrusion detection system. Others can be advanced tools such as data leak prevention, application security testing, database activity monitoring or automated vulnerability assessment tools (Lacey, 2013) [17].

As already mentioned, the system can use both basic technologies to increase the level of security, and advanced ones. Nevertheless, some points remain unchanged and necessary. The use of logs, which should be centralized and convey all the necessary information, all the basic security controls and SIEM to build the integrated SOC functionality (Lacey, 2013). Table 3 below is an example of security technology controls categorized as basic, advanced and APT specific technology controls (Lacey, 2013) [17].

Basic Security Technology Controls	Endpoint Antivirus, Gateway Antivirus, Firewall, Intrusion Detection, Penetration tests in corporate network, Strong authentication controls, syslog servers.
Advanced Security Technology Controls	Automated vulnerability scanners, Database security monitoring controls, Intrusion Prevention Systems, data leak prevention systems, Data diodes between Supervisory Control and Data Acquisition (SCADA) and corporate network, SIEM.
Specific APT Technology Controls	Web application firewalls, file integrity checking tools, Threat data feed into SIEM, advanced forensics, honeypots, Application whitelisting.
Best available practices	Security in Software Development Life Cycle (SDLC), Enterprise security architecture, information exchange forums, trusted computing.

Table 3. Security technology controls categories. Source: Babu Veerappa Srinivas

The SOC requires specialized applications besides SIEM and IT management software. These software tools include:

- Cyber threat intelligence databases and feeds
- Governance, risk, and compliance (GRC) systems
- Firewalls, including next-generation firewalls (NGFW)
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Penetration testing tools
- Vulnerability scanners
- Wireless intrusion prevention

It is not wise to cut budget corners when equipping the SOC. Your team requires a robust set of tools to achieve the multiple benefits a SOC can generate [16].

Step 2: Cyber Culture Management

The training of staff in dealing with such situations is considered vital. Staff training is a very important factor that needs to be expanded, staff training is a consistent and ongoing process based on culture, technological advances, new requirements and improvements to systems and any upgrades.

In the process of staff training there are processes for learning the systems, media, logging behaviors and operating rules, and the skills for the required actions that must be acquired at a critical time. Staff training should be oriented and cover specialized areas, general training should be avoided with the logic that they tire staff and secondly enrich their minds with knowledge that is outside of their department so in a critical moment is not immediate involved, as it does not directly concern their department. Specialized educational approaches are the ones that help a lot.

Should not overlook the fact that critical energy infrastructures need protection from physical disasters, for which reason the above revised training approaches should include non-structural vulnerability training, such as staff training on the proper placement of their offices. Ways and places of installation of the equipment, the appropriate configurations of the places, there should be the appropriate lighting in the place, the configurations with partitions in the interior places. Etc. Skilled staff plays a key role in defending the organization against cyberattacks (Homeland Security, 2013).

The personal security of both staff and industrial systems is categorized into two categories, the first category is called "active" and describes the means that should be used to deal with an emergency, the second category is called "passive", in this category is planned and the constructions required for the necessary protection are applied. Human resources should, for their own safety and the safety of the infrastructure, follow specific protection and response measures in accordance with the rules of operation of the infrastructure.

Staff training on personal security should also include methods of psychological protection and resilience of staff, which is of particular importance both during and after a hazard. They should not feel insecure and disadvantaged at the critical moment, instead they should contribute as they are trained, participate in the valuation process, participate in activities and actions throughout the risk phase, while they should be flexible in their approach redefining procedures. After the end of the risk, the staff re-evaluate the critical energy infrastructures, logging the damages, the functionality of the facilities, the suitability, and to the extent and which sectors cannot function, the evaluation of the above controls is not only intended to evaluate the present situation but also the future analysis and evaluation of data on the implementation of new security policies and infrastructure protection methods, including the physical security of staff, the protection of industrial plants, and the evaluation of better storage and protection of fine materials that could be harm human lives and the environment, such as chemicals, fuels, etc. Finally, the effort to restore the smooth operation of an infrastructure is a process that collectively affects all sectors, and should be carried out with a plan for dealing with and reactivating the infrastructure after a hazard.

Critical energy infrastructures need to be staffed with highly qualified and efficient staff, who have been properly and intensively trained in comprehensive training programs, are aware of their role, know how to exercise their responsibilities responsibly, are obedient to safety rules, and are finally able to contribute to the security of the infrastructure in the ways indicated to it by those who is responsible. The staff of a critical energy infrastructures should have a huge stake in the efficiency and security of the infrastructure, should ensure the processes and integrity of the infrastructure, should contribute to the further cultivation of the security culture, and contribute with its proposals when is asked, it will improve processes and safety measures which may have come to staff notice. Staff training should be carried out by accredited bodies and the training should be focused based on an appropriately designed training program which will be targeted according to the responsibilities of each sector in an infrastructure and depending on the specialty of the staff, the training includes necessary training of staff in critical security challenges which include the security of the premises, the security of the information systems, the security of the industrial equipment, the secure storage of sensitive information, the secure execution of the required processes, instructions for the personal safety of the staff, and finally ways of dealing with risks depending on the position of the staff and the responsibilities it has in order to carry out the processes that must be carried out to prevent a risk. In addition to the theoretical training, the practical training of the staff based on real virtual situations of intrusion of a critical energy infrastructure is necessary, in order to evaluate the performance of the security policy but also the readiness of the staff.

Finally, it is worth noting that in addition to the European Program for critical energy infrastructures Protection (EPCIP), which sets out some key operational and safety conditions of European critical energy infrastructures that are undoubtedly deemed necessary, it also mentions critical energy infrastructures assessment methods to minimize risks and threats. Regardless of the operating conditions of the European critical energy infrastructures, the critical energy infrastructures also need ISO certification to ensure its quality and level of safety, so there are the following standards according to International Organization for Standardization (ISO), which are based on the uninterrupted operation of the critical energy infrastructures, some of them are.

Of course, any information communicated on critical systems must be encrypted, control systems on industrial systems must be encrypted, critical energy infrastructures control operation commands must generally be encrypted. Encryption not only ensures the integrity of the information and goods produced, it ensures the consistency of the operation of the entire infrastructure, the confidentiality of the systems communication by adding another layer of security to the industrial infrastructure systems. Information is very important, for this reason the information should be used in accordance with the security policy, classified according to priority, and it should be specified which employee has access to the degree in the information. The human factor remains the number one threat, for this reason, the staff must sign a non-disclosure agreement, and secondly the staff must be limited only to the information needed to perform their duties.

Step 3: Organization Management

Disaster Recovery is a subset of the Business Continuity Plan as it aims to immediately address the malicious effects of a cyber-attack by eliminating its negative effects as much as possible, using methods of immediate recovery in the shortest possible time that industrial systems do not be affected. For the use of methodologies, an important factor is the available resources of the critical energy infrastructures; it is not understood Business Continuity Plan and Disaster Recovery Plan without available resources. Critical energy infrastructures systems need to properly manage available resources and release them when they are not needed. The available resources are crucial both in dealing with malicious intrusions and in the immediate implementation of the Business Continuity Plan. Procedures are therefore required to ensure that resources are always available to allow the immediate implementation of the Business Continuity Plan, without these available resources being affected by a malicious attack.

The security of the systems and their available resources in the critical energy infrastructures is a high priority as it is a very important entity, which is non-negotiable. In the field of critical energy infrastructures security, advanced technologies and techniques are applied in order to ensure the integrity of the production and the reliability of its operations. The communication of information systems and networks must function flawlessly without unnecessary loops and with full utilization of the available resources of the systems in order to improve their productive capacity and the integrity of the control and production operations. Information must be collected, stored and utilized in a secure and correct manner to prevent errors and mistakes. Maintaining the security of systems and networks in critical energy infrastructures is an important entity that never stops evolving. Instead, it follows the technological requirements of the time and complies with European and cyber security compliance guidelines. Systems in critical energy infrastructures must be able to receive and provide reliable information and control commands, authorized users have the ability to manage and control by sector, the information circulated is critical, as this information will then be analyzed, controls, changes in production, modification of functions, etc. There is no more or less secure information systems in critical energy infrastructures, all systems have the same weight and need the necessary security.

Preventive measures must always ensure the safety of staff and the integrity of the operation of the infrastructure, in no case should the operation of the infrastructure be restricted or the role because of an attacker be changed, otherwise for the above reasons The corresponding studies are carried out. It may be a good practice to seek out open-source information about impending studies of attacks and vulnerable industrial systems that may be published on the Dark Net on Onion Servers, or even studies published by universities on security issues of industrial and information systems of critical energy infrastructures. A detailed record of staff functions could reveal some vulnerabilities, as some function features could be identified that could possibly be used by external hackers or even internally by some employees who would like to intentionally create problems in the operation of the infrastructure.

The design of the right Business Continuity Plan presupposes some important steps, it is a process that presupposes important analysis and evaluation, presupposes the creation of some steps, which can be characterized as main points and are the main axes of dealing with and implementing specific measures. Proper design of a Business Continuity Plan presupposes key entities that need to be analyzed and evaluated before the rules and methodologies of systems recovery can be written, so the main points are:

1. *Systems evaluation and evaluation of objectives.*
2. *Risk Analysis.*
3. *Impact Analysis.*
4. *Design methodologies for dealing with the risks that have been evaluated.*
5. *Creation of a complete plan for dealing with and continuing the operation.*
6. *Evaluate the project with simulation to evaluate its degree of success and whether it can be implemented in reality.*
7. *Training of the staff involved in the plan for dealing with dangerous situations.*
8. *Check that the integrated response, business continuity plan, and data recovery complies with the security policy to which the infrastructure complies.*

In addition, an important factor is the evaluation of very critical and sensitive sectors of critical energy infrastructures, including communication and exchange methods given encryption algorithms, staff confidentiality to industrial systems, staff certification methods, management of critical industrial systems, and finally industrial production systems, and finally the effects of each of these entities if for some reason they cease to operate properly.

Additional control measures, isolation of threats in combination with Business Continuity Plan measures should be applied where necessary, in order to eliminate the risk of non-immediate response and proper assessment of the situation, which are formally documented in the critical energy infrastructures. These documents include identified weaknesses, reaction timeframes, recovery timeframes, processes, and staff responsibilities required to be done, as well as secure communication methods for all parties involved. An important precondition for the proper implementation of the Business Continuity Plan is its continuous evaluation, especially after any changes have been made to the critical energy infrastructures, in order to re-evaluate the situation and the effectiveness of the methods of continuation and repair of damages. The implementation of the Business Continuity Plan, apart from the prevention of catastrophes and the application of methodologies for the operation of the systems, also aims at the avoidance of waste of costs regarding the recovery of the damages after a cyber-attack. Cost is an important factor and often a negative example because due to the high cost, actions and evaluations are bypassed which should be done and implemented in order to improve industrial systems and protect critical energy infrastructures from significant future cyber-attacks. A compensatory factor of high cost is that technology is evolving rapidly, new possibilities are emerging resulting in the cost of implementing some capabilities and actions to be taken is reduced, certainly for some weak economies it may seem high while for some other countries it may seem ideal.

Critical energy infrastructures industrial systems need protection from cyber-attacks and support from automatic recovery systems that either are based on the very capabilities of industrial recovery systems or rely on other systems that act as supporting systems for recovery of main systems. An important entity in critical energy infrastructures is backups, backups as well as other infrastructure systems need security, and isolation from other infrastructure systems, a separate space properly configured away from other industrial systems is an appropriate shaped since backups may be adequately protected from either a cyber-attack or a physical disaster. The following must be strictly observed for the specifications of the backups:

1. *The specifications of physical storage and isolation of backups.*
2. *The possibilities of protection and physical preservation.*
3. *The security features against the most probable disasters.*
4. *The methods by which the backups will be stored and retrieved.*
5. *The encryption required.*
6. *The network isolation of backup systems from other systems.*
7. *Determine the temperature of the storage place.*
8. *Conservation of energy efficiency.*

In addition, there must be an operation plan in the recovery plan, i.e. which systems will work and how after an attack, how the staff will work and which systems are considered secure in order to continue the work of the staff and to continue the operation of the infrastructure. Specifically, the work plan must include the following:

1. *Identify trusted systems that can operate after an attack.*
2. *Which systems are considered secure after a disaster.*
3. *What methodologies need to be done for the systems to start recovering.*
4. *Identify systems that are able to recover automatically.*
5. *Identification of reliable systems that will work in case the main systems are out of order (backup systems).*
6. *Data network recovery procedures, if this is not possible, the creation of backup paths to the data network.*
7. *Uninterruptible power supply even in conditions of extensive damage.*
8. *Creating a plan that restores the operations of industrial systems in a very short time.*

Step 4: Resources Management

Critical energy infrastructures consist of sets of interconnected systems and industrial devices that work smoothly together to produce various goods that concern society and thus help it evolve and become more creative and productive, both society and the state. The more sophisticated a critical energy infrastructure is, the more sophisticated processes are performed, leading to an increasing number of complexities in assessing and predicting future hazards.

Risk management performed on critical energy infrastructures taking into account 3 parameters: Threat, vulnerability, impact. Particular emphasis is placed on the third parameter, which concerns the impact of an attack in critical energy infrastructures, how an attack can affect it and the impact it can have on society as a whole. In infrastructure related to electricity production and telecommunications, are applied methods oriented to the modeling and determination of interdependencies depending on the sector in which a critical energy infrastructure is involved.

Vulnerability assessment and subsequent patching of security vulnerabilities is a key strategic, critical and necessary for critical energy infrastructures. The assessment must be flexible and coordinated not only in the critical energy infrastructure systems but in the subsystems to assess whether they are vulnerable and how they will behave in the event of an attack. The "ring of defenses" security strategy, which is particularly prevalent in industrial systems, is the ideal choice to fully evaluate the industrial systems of critical energy infrastructures. The ring of defenses security strategy, as its name implies, is a ring that has layers, in each layer there are compensatory measures for the security of the infrastructure. These areas are mainly classified as follows:

- **First Level Firewalls (DMZ):** *It is the first level of security that aim to prevent attempts to illegally connect external IP addresses to internal information systems. Also, provide protection against denial of service (DOS) attacks.*

- **Second Level Firewalls:** *Ensures the prevention of external and internal users connecting to other systems and services that are not allowed. In addition, at this level non-authorized users protect connection to File Servers and Databases. Finally, it defines the communication rights of applications and IIoT in the infrastructure network.*

- **Proxy Servers:** *They are network servers located within critical energy infrastructures; their purpose is to provide a level of security to network applications, software, automated systems, and mechanism controls. The use of proxies provides an extra level of security as infrastructure systems they can only communicate through the proxy server, so a security method is applied where in order to communicate one system with another one must know in advance the authentication credentials of the proxy server.*

- **Operating Systems:** *Infrastructure operating systems must be adequately up-to-date, in accordance with security policy, and always be behind network security systems. Each computer system should be evaluated individually if it meets the security specifications and its security vulnerabilities should be fixed according to the security policy and not just because a new version of a service pack is available, as a new version of a service pack may change the policy. or offer new features to users by modifying the system vulnerably, so needed to evaluate before installing new security updates on operating systems.*

- **Software:** *As mentioned in previous chapters, the field of software security is complex, involves the security of application functionality by applying security levels of the developing application at each stage of its implementation, also presupposes the creation of immediate software recovery mechanisms in case of a cyber-attack, the metadata of the applications are of particular importance and need the protection and encryption that they deserve. Both the application's security managers and the company that developed it to improve areas that need improvement as well as to identify potential security vulnerabilities to eliminate must constantly evaluate critical energy infrastructures software. Software in critical energy infrastructures should in no case be used as the sole authentication point without the use of other network protection methods, and should always be under the protection of security equipment.*

- Policies: *This is a security policy; it lists all the features and methods of security and countermeasures. Includes report analysis, ways of security of information and industrial systems, prerequisites, guidelines, etc. It is necessary for any critical energy infrastructures, without the existence of security policy, there is NO security in the critical infrastructures and the critical energy infrastructures operates with a very high operational risk, the staff does not know how to react at a critical moment, while industrial production is in danger.*

- Critical Sector: *It is the heart of critical energy infrastructures operators. This is an isolated sector, which is surrounded by control and security mechanisms. It provides a high level of security, but there is no 100% security anywhere. Security mechanisms include a Firewall to control incoming / outgoing connections to other mechanisms. An Air-Gapped network with separate IP addresses isolated from the rest of the infrastructure network is used. The purpose of security is to prevent all unauthorized users / attackers from accessing this isolated network in any way, security vulnerability and risk assessment methods should focus on techniques such as* ***IP spoofing*** *and the use of* ***ARP*** *protocol.* Security checks on operating systems in this critical sector are a top priority, and regular checks for security vulnerabilities in critical sectors may reveal several vulnerabilities that need to be addressed. Finally, staff management mandates in particularly critical sectors must be certified by other certification and verification methods. The right security policy combined with blocking security vulnerabilities will not expose particularly critical areas of the infrastructure to risk; the right configuration is what will prevent possible connections to systems that should not be allowed.

  There are 3 key factors on which critical energy infrastructures must be based.

  1. *Definition of basic prerequisites for the security of all infrastructure systems including goods.*
  2. *Efficiency of the security systems, which are available, with vulnerability assessment.*
  3. *Analysis between implementation costs / damage recovery costs.*

Identifying and evaluating security vulnerabilities is recognized as a potential threat to infrastructure information and industrial systems, as well as their available resources. European infrastructure must apply the necessary characteristics and practices as defined in relation to the protection of critical European infrastructure. A security vulnerability check may be used for security systems performance as defined in the security policy specifically a security vulnerability check may be useful for the following reasons:

1. *Evaluation of countermeasures and contingency plan.*
2. *Evaluation of staff in terms of their roles and responsibilities.*
3. *Capture the security status of the infrastructure.*
4. *Corrections, patching and other interventions required.*
5. *Timely detection of security vulnerabilities and their management before being detected by a Hacker.*
6. *Evaluation assessment depending on the infrastructure sectors, which sectors need more security.*
7. *Evaluation of protection of the produced goods.*

Step 5: Strategy Management

For the security of critical energy infrastructures and beyond, security models have been developed that analyze security prerequisites under different circumstances and determine future action plans and security policy that is often adapted to the needs of the time. Using models of future predictions can be approached the probability of a cyber-attack by determining the moment. The aggregate distribution function can determine the probability of stochastic attacks, as they can be determined based on the range of values, less than or equal to a given segment, with the help of various functions it is possible to determine the spread and intrusion speed. Cyber-attacks utilizing the linear equations they can be represented, logging all the characteristics of the variables and all their measurements so that these elements may then be used by using successful prediction models and using probabilities to estimate the effect of the attack. The use of models in combination with the adoption of techniques is used to create transition profiles of events collected during the smooth operation of the infrastructure. The activities of the evaluated systems are analyzed in order to then calculate the possibilities of intrusion under normal operation of the infrastructure systems. Analyzing each function that is, putting each function under monitoring. The chances of activities are to determine the malfunctions, security vulnerabilities, operational errors and the extent of cyber-attacks. "Queueing" models are used for the effect of DOS attacks. The "Markov Chain" model is used to analyze the probabilities of metric performance, loss of interfaces, loss of buffer usage, etc.

The logging of entities in critical energy infrastructures must be done in terms of system requirements, which must be classified into two categories, the first category being security privacy, and the second category being critical security.

In security models, security properties can also be expressed as variables, so it can be determined if the systems will enter an insecure state at the critical moment of the cyber-attack. In this analysis, it is useful to represent the scenario by presenting graphs,which are able to represent the possible violations which could occur in the infrastructure. In addition, with the use of graphs it is possible to present the cases, which could violate the information and industrial systems of the infrastructure and in what ways. Finally, the use of the Markov model helps significantly in the representation of events during the operation of the systems. The activities evaluated during the operation of the systems are analyzed to calculate the chances of intrusion during operation. Low probability of activities is equivalent to the scenario of malfunctions in the systems from cyber-attacks.

Using prediction models, it is possible to represent all the involved sections by analyzing the chances of intrusion or attack by section by examining all the parameters evaluating each correctness, condition, and entity.

The logging of entities in critical energy infrastructures must be done in terms of system requirements, which must be classified into two categories, the first category being security privacy, and the second category being critical security. There should always be the thought that in the event of an intrusion, the intruder will never have access to the IT and industrial systems of the infrastructure will never have administrator rights, and finally, a damage or sabotage at some point in the infrastructure network will not affect the smooth continuation of infrastructure operations. In security models, security properties can also be expressed as variables, so it can be determined if the systems will enter an insecure state at the critical moment of the cyber-attack. In this analysis, it is useful to represent the scenario by presenting graphs, which are able to represent the possible violations, which could occur in the infrastructure. In addition, with the use of graphs it is possible to present the cases, which could violate the information and industrial systems of the infrastructure and in what ways. Finally, the use of the Markov model helps significantly in the representation of events during the operation of the systems. The activities evaluated during the operation of the systems are analyzed to calculate the chances of intrusion during operation. Low probability of activities is equivalent to the scenario of malfunctions in the systems from cyber-attacks.

The requirements of critical energy infrastructures systems are divided into two categories, the first category is the security of infrastructure information systems, and the second category is the security of critical energy infrastructures sectors. The first category, which concerns information systems security, suggests that nothing bad is going to happen that will affect the operation and integrity of systems, data networks, and infrastructure information. The representation of the above details can be presented using a graph, representing the entities with variable values. It is essentially a script that represents security and breach properties by incorporating parameters that could lead the system to an unsafe state. The safety of critical energy infrastructures sectors indicates the safety of industrial equipment including the critical requirements regarding the integrity of its operation. In critical energy infrastructures networks, data network security must be further evaluated against individual vulnerabilities that have been published. Critical energy infrastructures use a variety of ways to control their units, which means that all critical sectors need to be scrutinized in detail. In controlling the security of information systems and critical energy infrastructures networks, the effects of interactions must be taken seriously. All systems must be thoroughly checked for any vulnerabilities, and then these elements can be analyzed in conjunction with other elements from the network and applications. The above elements will lead to the creation of attack graphs; each part of the graph also marks security vulnerabilities that need to be fixed. It is possible to analyze each vulnerable part of the graph in terms of determining the size of the intrusion in terms of the influence on the systems. Any security vulnerabilities encountered are an element of attack. An attack tree can be created that can show the path that an intruder will take until it succeeds in breaking a system or the target system, it can present the techniques that will be used to reach an intruder on the target system, and finally the representation of the attack in the form of a graph which represents the process of intrusion. Attack trees help to present the security situation by presenting procedures that step by step describe how a vulnerable system can be compromised, including the nodes. Attack graphs have the ability to represent future attack scenarios, the term future attack scenarios do not invalidate the philosophy of attack graphs, thus creating penetration scenarios with the intruder steps, possible target paths, intersections, systems that are affected, and finally the user rights that may steal and use to access other systems and databases. In critical energy infrastructures, attack graphs can be classified into those that show the state of infrastructure information systems, attack graphs that show the state of critical parts of critical energy infrastructures, and finally, graphs of attacks that use future scenarios. Predictive and security models including attack graphs are used to determine the degree of vulnerability of infrastructure systems that need improvement or an enhanced level of protection, as they are able to highlight vulnerabilities that are combined with capabilities and The degree of influence on infrastructure systems. Prediction models are applied taking into account the following characteristics:

- *Detecting security vulnerabilities that have either not been detected in the past or have been detected in the past but have not been fixed.*
- *Determining the installation of new IDS, or modifying existing ones, the evaluation is based on analyzing the coverage rate and depending on the security needs that may have changed.*
- *Appropriate configurations in both hardware and security software, in accordance with the security policy.*
- *Communication network upgrade studies, in accordance with security standards and based on security policy. The upgrade of telecommunications equipment must be implemented where is required by faithfully following the rules of replacement and updating of networking equipment.*
- *Implementation of safety assessment scenarios, elaboration of worst-case scenarios and analyzing of the result for evaluation and compliance.*
- *Analysis of telecommunications equipment by capturing the advantages and disadvantages of the implementation of the present structure, the analysis of the waste will present compliance proposals where required.*
- *Assessment of security systems in critical energy infrastructures systems.*
- *Analysis of information from open source of* ***non-friendly countries*** *research or case studies on critical energy infrastructures security may reveal research into the analysis of software used in critical energy infrastructures, including security methods, mechanism controlling security levels to trigger a future intrusion.*

Creating attack graphs presupposes knowledge of the telecommunications network topology and systems in critical energy infrastructures.

A smart grid in critical energy infrastructures must be adequately protected against external factors. Despite the convenience and reliability, it offers, there are also security challenges that accompany it. An important pathogen of smart grids is that they integrate information into the network with all that entails for security issues as this network uses both communications of industrial equipment and all digital devices making it vulnerable to cyber-attacks and malware infection. A targeted attack on an smart grid is aimed at intercepting sensitive information, intercepting personal data, and finally intercepting automated industrial operations. As mentioned above, smart grids must always be in critical energy infrastructures, always adequately protected because they have the ability to interact with other smart devices such as IIoT. Inadequate configuration on smart devices that interact with the smart grid can be a gateway for intruders to the smart grid, Finally, coordinating all the operational teams involved in an industrial critical energy infrastructure is an important advantage as it can significantly improve communication within the infrastructure and at the same time avoid decisions that will lead to vulnerable systems in the future.

In conclusion, the success of smart grids is based on the proper installation, use, and operation of all the teams involved in a critical industrial infrastructure, which teams are able to solve any problems that may arise.

Studies on security strategies and improvement of existing systems are based on an approach theory called "game theory", in which block chain models are integrated into multiple levels of programs, these programs are also known as" Leader - follower". The hierarchical optimization problems where both the leader and the follower want to optimize their position at the same time, while the follower's solution is the reaction to the leader's solution. Critical energy infrastructures must apply optimal protection in such a way as to significantly reduce the rate of information loss and process failure.

As a model for identifying recognition practices for the protection of critical energy infrastructures systems, it is useful to use the r-Interdiction Median Problem with Fortification (RIMF) model, which is an extension of the RIM model, as a tracking model for identifying protection practices of critical energy infrastructures systems. For the implementation of the protection model is divided into two categories, the external category which models the decisions of the defenders and the internal category which detects cyber-attack scenarios based on a given protection strategy.

Both analyzing and capturing problems is a process that distorts reality, as it captures malicious actions, cyber-attacks, and physical attacks such as physical disasters which without the use of predictive models would be uncertain thoughts about the future which with the passage of the time would be repeated without clear indications of events that would follow.

The prediction models used to predict future threats to critical energy infrastructures unfortunately do not provide 100% accurate prediction of threats, but they do provide largely satisfactory forecasting for security studies, which largely repel future attacks. Predicting threats from a single model is not enough, so more than one combination of prediction models is used, choosing a single threat prediction model can lead to ineffective future security strategies and entail security measures as not all threat and vulnerability scenarios are taken into account.

Step 6: Security Management

To evaluate the management of control information that is communicated within a critical infrastructure, typically is used the **Plan-Do-Check-Act (PDCA)** method, which is based on the **ISO 27001** standard with which critical energy infrastructures are complied. The **Plan-Do-Check-Act (PDCA)** method consists of **4** phases. These **4** phases are intended for the **correct logging of functions, the analysis of information, the objectives set by each sector, the measures to be defined, the actions and any corrections that need to be made**. The implementation of the **Plan-Do-Check-Act (PDCA)** method is an important process, which during the start-up process records the security requirements and as an output describes the security procedures that need to be implemented or improved. The **4** phases are described below.

1. **Plan:** C*ollection and analysis of control information, the security methods of information, the logging of the objectives of each sector, the ways and methods to be applied.*
2. **Do:** *Creation of implementation rules of the measures that were collected during phase 1 above.*
3. **Check:** *Control analysis between the collected information, the objectives and the results.*
4. **Act:** *Application of results. Improvements, making the necessary modifications.*

Using the **Plan-Do-Check-Act (PDCA)** method, a critical energy infrastructure can assess the level of security of its sectors by separating the most critical and the least critical sectors in order to reduce the risk to acceptable levels. The use of the **Plan-Do-Check-Act (PDCA)** method aims to capture the security needs of the infrastructure and assess the risk taking into account the operational damage that the infrastructure will suffer if it is attacked by a cyber-attack. The resulting waste will contribute universally to the risk assessment for the implementation of appropriate methods and actions and the determination of prioritization. The **Plan-Do-Check-Act (PDCA)** method is not a one -time process, but a process that is repeated at regular intervals to **continuously assess risk, identify needs, re-evaluate any changes have been made, and to counteract any changes to the facilities and security policy** in order to be in direct compliance with the security requirements of the infrastructure and to protect it from new threats by reaffirming security measures.

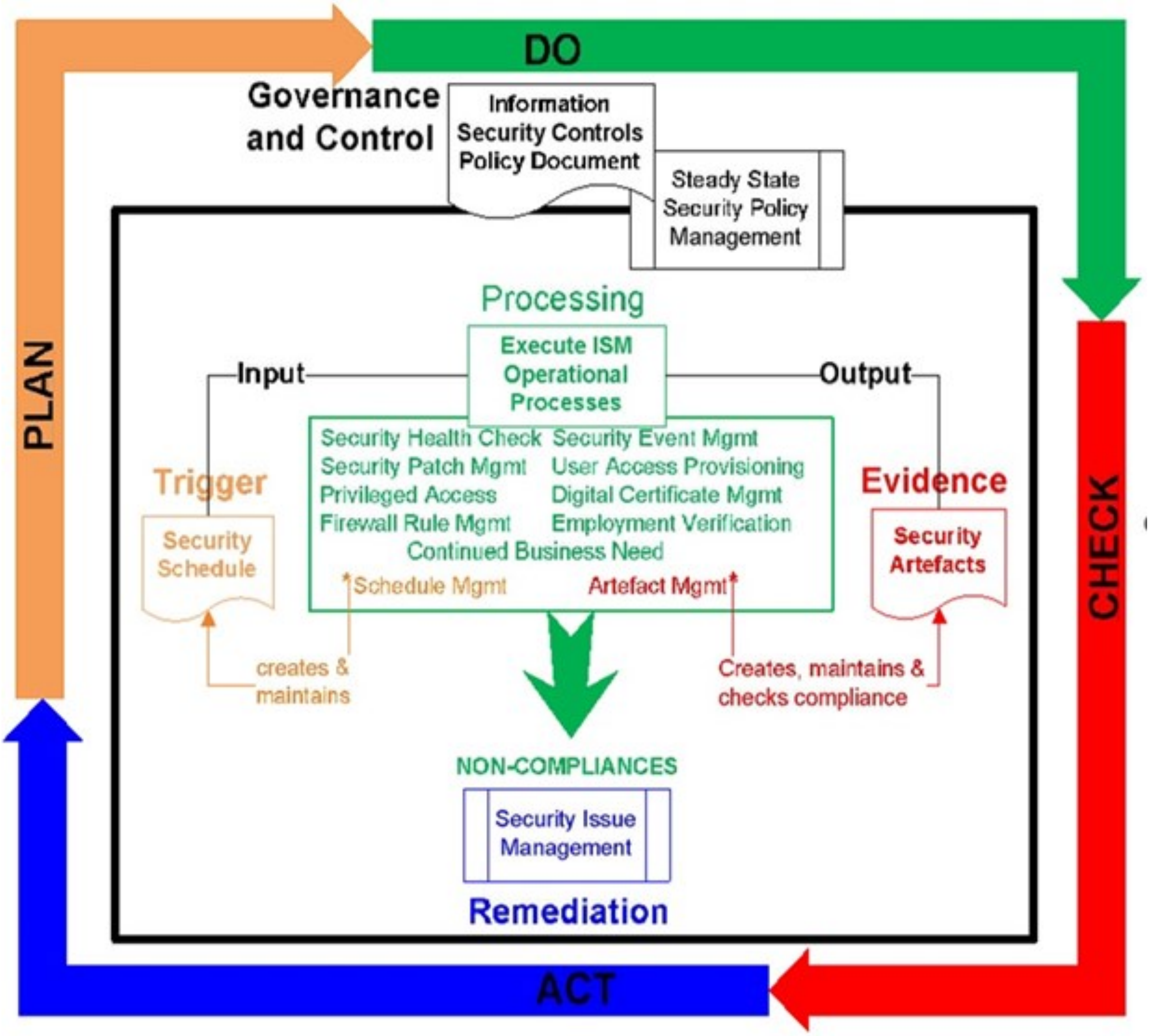


Figure 5. Plan-Do-Check-Act methods operating principle. Source: IBM Corporation

Either critical energy infrastructures have the ability to interact with each other directly or indirectly, this means that a critical energy infrastructure can access another critical energy infrastructure located in another city or another country. In this case, the integrity of the communication and the confidentiality of the transmitted information must be ensured, therefore an increased security layer is required as a particularly increased attention is required as a connection to a critical energy infrastructure is capable of affecting functions and systems of another infrastructure. it should be ensured that the information being exchanged is adequately encrypted and that no information is intercepted by a third entity (Man in the Middle Attack) that is capable of stealing sensitive operational information. Therefore, the exchange of operational information between two or more critical energy infrastructures should be based on a strict information exchange policy based on cryptography, European standards of confidential communications, and information authentication procedures. As mentioned in previous chapters, the application of the ISO 27001 standard applies to critical energy infrastructures, there are several sets of standards that critical energy infrastructures must apply to achieve a high level of security of their operational information, which implies increased infrastructure security.

Critical energy infrastructures industrial systems to work uninterruptedly, there must be mechanisms for incidence response to the threats, so that the threats are cut off and the systems continue to operate uninterruptedly, in particular, the following actions are required:

1. *Infrastructure security officers shall be informed promptly of any malicious activity occurring in the infrastructure network.*
2. *Procedures that are accurately described in the security policy are applied.*
3. *The staff applies the practices for which it has been trained.*
4. *The staff is limited to its responsibilities for its sector, performs the procedures for which it has been trained for responsibilities related to its sector.*
5. *Investigation for other incidents in the infrastructure.*
6. *General assessment of the situation and informing the security officials.*
7. *Start of a plan for the continuation of operation and continuous evaluation of the situation.*
8. *Evaluation of available resources.*
9. *Evaluate a follow-up plan taking into account available resources, threat elimination, and the likelihood of disaster.*
10. *Implementation of systems recovery plan.*

The ineffectiveness of dealing with a threat to critical energy infrastructures is determined by different parameters taking into account the correct security policy, which includes security and countermeasures, combining the above to see if what has been described has been properly implemented at the right time. For these reasons, there are various factors, which include:

1. *The real identification of the threat. The staff who will be called upon to deal with a threat to their field should be able to properly assess the level of risk, use the methods and tools needed at the right time to formulate compliance requirements accordingly with their security policy and training.*

2. *The actual risk assessment by the staff is particularly critical. A greater risk can be underestimated, if underestimated then the damage that can be caused will be greater. As methods of attacks and threats are eliminated, security measures must be eliminated along with staff training and knowledge must be improved.*

3. *Security vulnerabilities should be patched and not overlapped by different methods and practices. Violation of a security system that protects another vulnerable system very easily leads to an escalation of attacker's rights with unpredictable consequences for the infrastructure, including the rawness and quality of the products produced. Instead of overlapping measures, integrated security measures are proposed that presuppose the closure of security vulnerabilities where there is a combination of security measures that include physical security of systems, security of communication networks, and security of information and industrial systems.*

4. *The ease of use of incidence response measures justifies the effectiveness. A series of complex procedures are naturally overlooked or ignored by staff for a variety of reasons, with the simplest reason being that an employee forgot the series with the huge procedures had to follow. The aim is to implement the appropriate deterrent at the critical moment. They must countermeasures not to commit sufficient resources given that the resources available at the critical moment are valuable. In addition, the application of countermeasures should not affect the operational activities of the infrastructure. Therefore, efficient and deterrent functions are needed in combination with the ease and speed of their implementation by the infrastructure staff.*

Software who is under development for critical energy infrastructures requires thorough checks on its functionality, if it meets the needs for which it was created, if its user interface is operational to users, and finally if the software can be completed successfully some stages of security controls. The software must successfully pass the security test by recording its reaction during the evaluation process through a list of specialized test attacks. This process is necessary because the test results will highlight the software security level, as well as any deficiencies in specific security standards that are essential for software intended for use in critical energy infrastructures. There are specific methodologies that must be followed to perform clear and valid results. The evaluation of the security of the software with the necessary control mechanisms is a key element of the security of the critical energy infrastructures systems and is enshrined in the security policy of the critical energy infrastructures as a basic precondition for the operation of software in the infrastructure facilities. Risk assessment processes are linked to threat modeling processes in conjunction with risk analysis.

Software that has not been evaluated and has not successfully passed the reliability checks should not be used in critical energy infrastructures, the reason is that this software may behave in an unexpected way, this is an unacceptable phenomenon. There is no exception to the above rule for information systems and in general for software running in Air-Gapped environments. Critical energy infrastructures security policy must be taken into account by software developers in terms of both software controls and the security features that will be implemented in the software who is under development.

A secure and operational software intended for use in critical energy infrastructures presupposes the following entities:

- *Detailed recording of the conditions, taking into account each safety parameter.*
- *Security is a process that involves the development of software at each stage of its implementation, taking into account each parameter.*
- *The software who is under development must fully meet the requirements of the security policy, to be able to continue its operation even during the process of an attack.*
- *Implement the certifications required for software development. Software functions must respond promptly and use resources in the most efficient way.*
- *If the software who is under development after an attack fails to recover, loss mitigation mechanisms should be included, separating the system into operational areas.*
- *Software that covers a wide range of functions should not be created, software that covers a wide range of actions is more prone to attack and complex both in handling, in development and maintenance.*
- *Important information should be kept secret, using control mechanisms and information encryption.*
- *Protection against internal attacks, easily an unhappy employee could cause an internal malfunction problem, the software who is under development should include management mechanisms taking into account that the user who executing commands may not be so confident, so a second validation method to executed commands is required.*
- *Non-certified software that does not meet safety requirements and is not certified for use in critical energy infrastructures cannot be used in critical energy infrastructures.*
- *Software should not be used as the sole means of authenticating users, systems, processes. A certification control mechanism must precede the software control mechanism.*

All of the above entities are essential.

Pre-made templates are directly related to software quality assurance, there are two types of pre-made templates that are classified either according to the description of the software components or based on software development processes. Pre-made templates based on the description of software components present components of software categories of the same categories pre-made templates based on software development processes include software application implementation processes that apply to critical energy infrastructures. Proper use of pre-made templates aims to produce certified software of high standards and quality, which without the use of pre-made templates is a complex and time-consuming process. The whole process of software analysis and development based on pre-made templates must be documented in writing, creating documentation. These documents cover the entire process of software analysis and development throughout its implementation phase, the documentation must be accurate in their descriptions and understandable so that in the future the software upgrades and extensions will be fully understood. Therefore, documentation apply a structured sequence of records, which is unique and prevents differences in the writing of documentation records of different or missing items. Therefore, they must have the following characteristics.

- *Detailed description of the procedures and processes that have been followed.*
- *How they were implemented and their purposes throughout the software development phase.*
- *The purpose of the software implementation.*
- *Description of pre-made templates related to the operating standards of the systems involved.*
- *Description of software requirements and analysis.*
- *Description of security methods related to infrastructure security policies.*
- *Reports of disputes and how they were dealt with.*
- *Software control plan reports.*
- *References on quality assurance.*
- *Stakeholder reports.*
- *Source code references.*
- *The possibilities of acquisitions and configurations.*
- *Deliverable user manuals.*

Undoubtedly, the implementation of certified pre-made templates loosens hands in the development of complex and secure software applications of critical energy infrastructures. Pre-made templates are created by scientists who have experience in specific areas, as well as software development experience that is bug free and meets automation needs that would require thousands of lines of code to solve. In addition, their quality is guaranteed, which implies security and execution of complex processes both during the software development process and the capabilities of the software produced. The use of pre-made templates significantly reduces implementation time, as no extra certifications are required for the software who is under development. The main goal in software development in critical energy infrastructures is to achieve a high level of quality, functionality and security. For these reasons, the correct choice of implementation methods is determined during the software design and development process.

PART III: HOW TO CREATE SOC (TECHNOLOGY)

How to create a security operations center (SOC) (technology)

SOC (Security Operations Center or Security Operations Center) is what unites people, processes and technologies in achieving a global goal: reducing risks through increasing cyber protection in an organization. Above all, the SOC is a team of security experts armed with technologies to detect, analyzes report and prevent cyber threats.

SOC can be compared to the work of a team of firefighters or paramedics on an ambulance. Cyber specialists in the SOC, like emergency workers, help in an emergency: they quickly appear in the right place, analyze threats and respond appropriately. They are also united by the desire to prevent such incidents.

SOCs are continuous streams of information that are processed by both computer systems and experts.

After choosing the SOC functions, it is necessary to proceed to the development of a target model that defines its main components in the context of the classical triad "personnel-processes -technologies" (Figure 6).

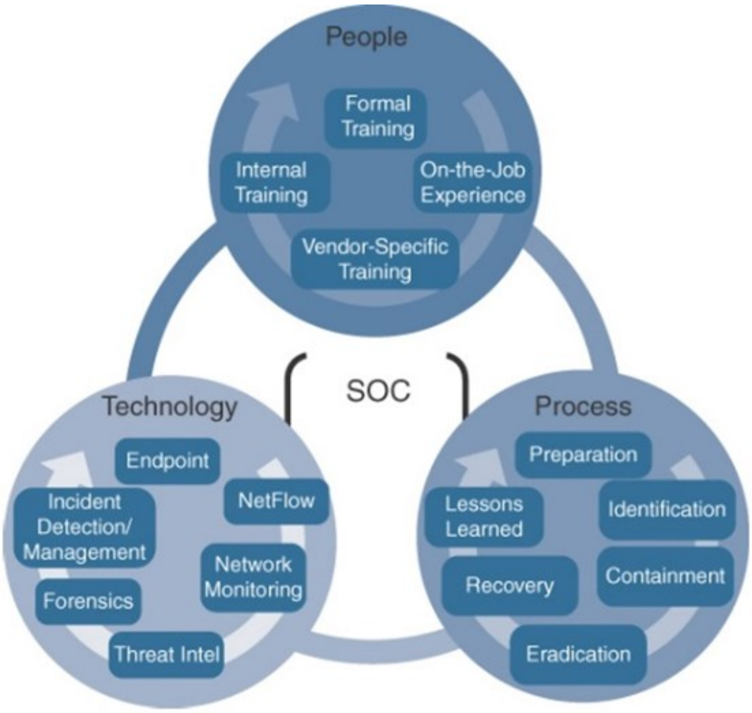


Figure 6. People, process and Technology Core Elements. Source: Joseph Muniz

SOC model helps to decide:

1. what processes are needed;
2. what technologies are required for process automation;
3. what personnel is needed to implement processes and support technologies.

There is no correct formula for the composition of SOC. Everyone has their own path and their own “mandatory” set of SOCs. The composition very much depends on the functions of the SOC and the volume of tasks it solves. Therefore, several issues need to be addressed during the development process. First, how will the SOC provide security? For example, will SOC-like functions be performed by a small-dedicated SOC team, or is the audience so large that the SOC's hierarchical structure makes more sense when SOC functions are spread across multiple teams? [15]. The next issue is the distribution of personnel depending on the functions performed by the chosen model. In other words, how functions will be translated into personnel roles and organizational structure [15]. As already mentioned, there is no single SOC structure that fits all organizations, so they can be combined. Appendix 3 presents in tabular form the main structures of the SOC organization, as well as issues related to SOC procedures. This table is a template that can be used when organizing a system SOC.

Step 1: Process

A common mistake when creating SOCs is the wrong alignment of processes: often the documentation that regulates them turns out to be unviable and “leaves the table”. As a result, specialists armed with technical means are left without a clear understanding of the tasks facing them and without detailed instructions for their implementation. In such conditions, it is extremely difficult to organize productive interaction within the SOC and with related departments.

For the effectiveness of the SOC, it is recommended to model the processes of the control level and the operational level. The first ones will help to ensure its development and a given level of quality for the implementation of the main functionality. The second ones involve building the main (i.e., directly related to the implementation of the target functionality) and auxiliary processes. The latter serve to determine approaches to connecting event sources, developing correlation logic, solving troubleshooting problems, and updating the list of information assets in the field of monitoring and data about these assets (Figure 7).

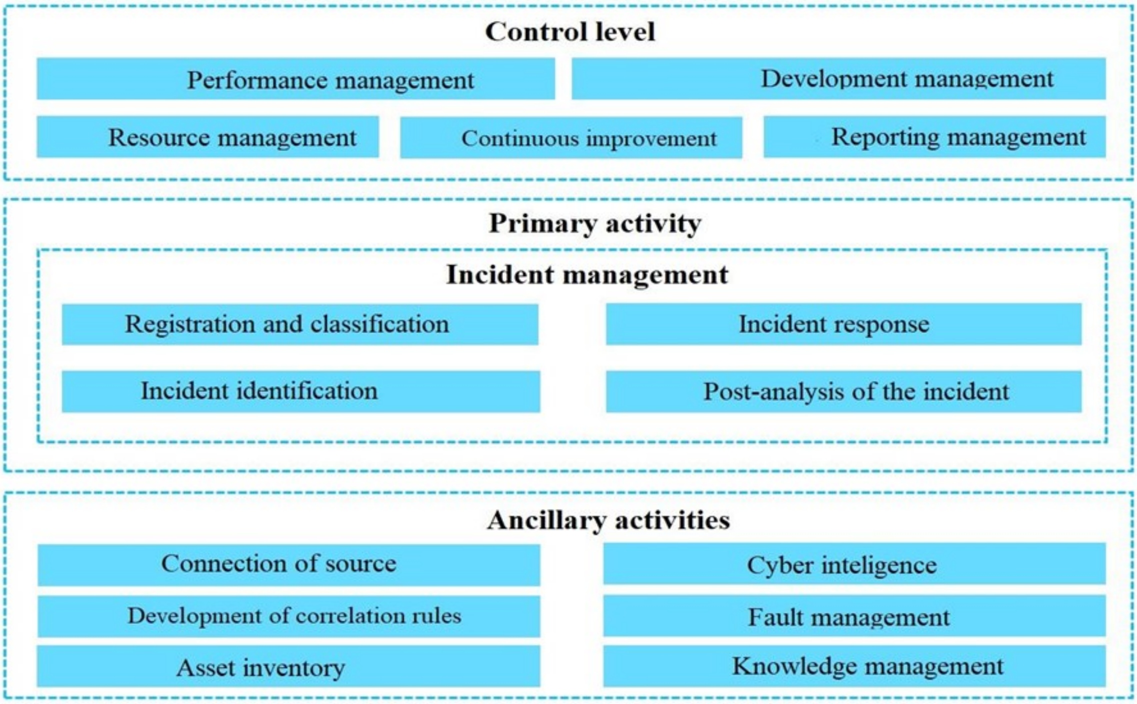


Figure 7. Generic SOC Process Map. Source: author

The need for any SOC function to protect systems at first glance should be decided in the same way as the need for any other measure of protection: based on a risk assessment. MITER offers a slightly different approach based on the size of the organizational unit that performs these functions. Annex 3 discusses several types of SOCs based on economic and managerial feasibility. Depending on this, for each function it is determined whether such a function should be implemented in full, partially, or if it is optional. Annex 4 shows the dependence on the type of SOC of almost all the functions that the system can perform. An example of the dependencies of some functions are presented in the Table 4.

Name	Virtual	Small	Large	Hierarchical	National
Real-Time Analysis					
Call Center	O	B	A	A	A
Real-Time Monitoring and Triage	O	B	A	A	O
Intel and Trending					
Cyber Intel Collection and Analysis	B	B	A	A	A
Cyber Intel Distribution	O	B	A	A	A
Cyber Intel Creation	-	O	B	A	A
Cyber Intel Fusion/ Trending/	O	O	A	A	A
Threat Assessment	-	O	B	B	A
Incident Analysis and Response					
Incident Analysis	B	B	A	A	O
Tradecraft Analysis	-	O	A	A	O
Incident Response Coordination	B	B	A	A	A
Countermeasure Implementation	O	O	O	O	O
On-site Incident Response	B	O	O	O	O
Remote Incident Response	B	B	A	A	O

Table 4. Example of some function’s dependencies on the type of SOC. Source: Carson Zimmerman, author

First, the SOC must analyze events and information security tools to identify incidents. This must be done not only in real time, but also for a given period of time in order to detect missed incidents. To ensure that the incident does not recur, it is important to analyze the results of the response. It is necessary to understand why the incident occurred and how effective were the measures to eliminate it. Tracking the values of metrics makes it possible to identify and eliminate problems in time, which can be both in the organization of the process and in the personnel implementing it. SOC activity analytics is displayed in the form of various tables and charts. The basic principle of operation of the SOC system is shown in Figure 8.

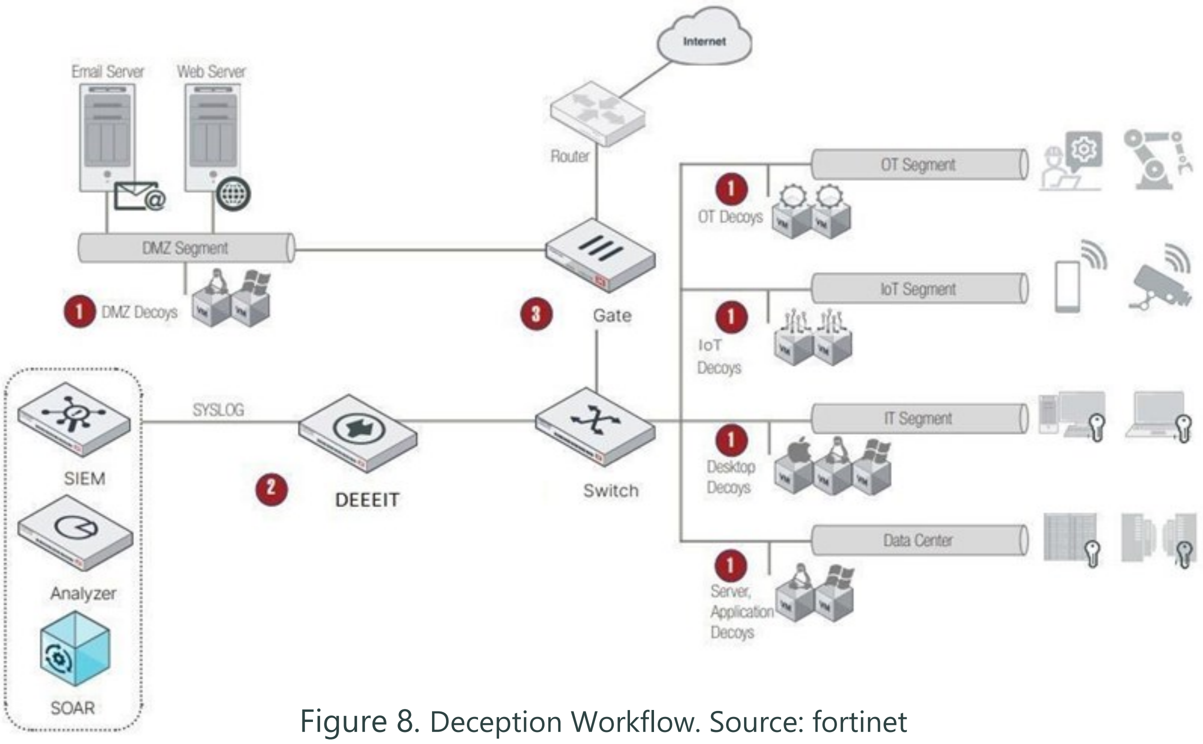


Figure 8. Deception Workflow. Source: fortinet

1. First block - controls, analyzes and filters external connections, creating active traps and fake resources, simulating the constant work of real users, software and hardware systems. Attackers successfully attack them, achieving imaginary results of the attack, which gives the SOC team time to respond. It also controls, prohibits or allows access from the internal network.

2. Second block - this block consists of three systems: SIEM, SOAR and Analyzer, which automate the detection of incidents and tasks for their processing, by collecting, correlating and analyzing events and information protection tools, analyze traffic, increase the speed of incident response and encode data. In addition, these systems can perform additional tasks: inventory and control of IT infrastructure, vulnerability management, prioritizing vulnerabilities according to the levels of criticality of information assets, automatically assigning responsible persons and deadlines for elimination.

3. Third block - network traffic monitoring, accounting, control and differentiation of user access from within the network to external resources, support for deep inspection of packets with checking for belonging to an existing connection, malware and attack detection, file and application control, email filtering and spam protection, intrusion prevention, load balancing, fault tolerance, etc.

How to avoid mistakes when building SOC processes:

- Connect all interested departments to process modeling;
- Fix the areas of responsibility of specialists and determine the most convenient channels of communication between them;
- Conduct pilot testing based on simulation results;
- Conduct training for all those who will be involved in the implementation of the processes, with the analysis of real cases;
- Develop a set of metrics to evaluate the correct functioning of the process.

Step 2: People

The work of a team of security experts depends on the organization, its goals and needs. This could be a security team, a permanent team within the organization, an external team of IT and cybersecurity professionals, or a combination.

The Security Operations Center should employ qualified and certified personnel. Since problems and threats are constantly changing, you need people who learn quickly, adapt easily and can think outside the box where you need to make quick decisions. It is best to involve current employees from the IT department in the SOC.

To implement the basic functionality, the SOC team needs to include specialists who will solve the following tasks:

- monitoring of information security events;
- registration and classification of suspicions of an information security incident;
- collection of the necessary data to analyze the suspicion of an information security incident;
- analysis of suspicions of an IS incident in order to identify it;
- coordination of response to information security incidents;
- administration of SOC technical tools;
- development of SOC infrastructure.

The main team should be formed as early as possible so that it participates in the implementation of systems and debugging processes. A good background for a SOC employee is experience in administering IT systems and network infrastructure, implementing and administering information security, as well as skills in conducting penetration testing. Do not forget that the staff must have not only work skills, but also the appropriate certificates:

- 1-CISO (CISSP, CISSM)
- 1-SoC Manager / Team Lead (CISSP, ISACA IT Risk, GIAC).
- 3-Level 3 Threat hunting (CEH, Pentesting, malware reverse engineering)
- 3-Level 2 Incident respond (CEH, GIAC: GCFA / GCIH)
- 6-Level 1 Analyst alert (GIAC: GSEC / GCIH /GCFE)

In addition to informational messages from IT and information security systems, SOC must promptly process requests and calls from users, messages from various departments of the company, information from external sources, etc. Figure 9 shows SOC role model example.

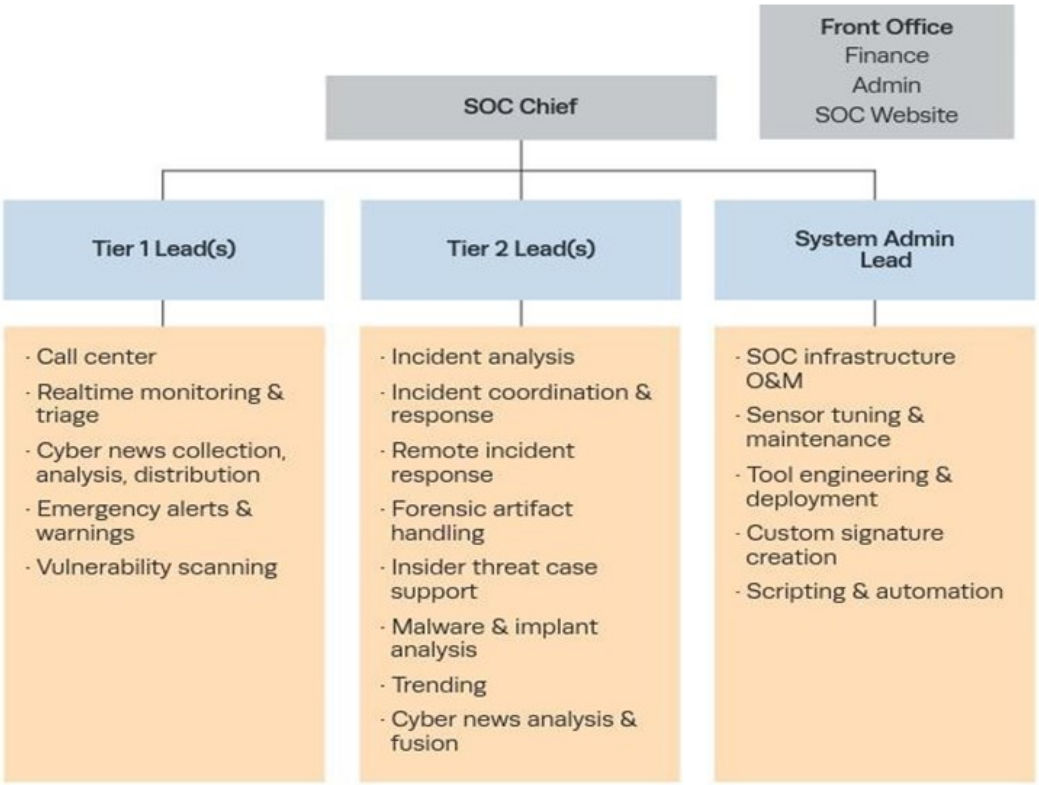

Front Office
Finance
Admin
SOC Website
SOC Chief
Tier 1 Lead(s)
Tier 2 Lead(s)
System Admin Lead
· Call center
· Realtime monitoring & triage
· Cyber news collection, analysis, distribution
· Emergency alerts & warnings
· Vulnerability scanning
· Incident analysis
· Incident coordination & response
· Remote incident response
· Forensic artifact handling
· Insider threat case support
· Malware & implant analysis
· Trending
· Cyber news analysis & fusion
· SOC infrastructure O&M
· Sensor tuning & maintenance
· Tool engineering & deployment
· Custom signature creation
· Scripting & automation

Figure 9. SOC role model example (Small SOC). Source: Carson Zimmerman

To process incoming information, recommended to create a first line group. It will ensure the analysis of incoming data and the selection in the general stream in accordance with the accepted policies of data indicating an information security incident. First line specialists do not carry out an in-depth analysis of the incident, their main task is to promptly process incoming information (watching IDS or SIEM consoles). If the incident takes more than a few minutes to process, the incident should be escalated to the second line of the SOC.

All incidents with a high level of criticality are also subject to escalation. The delay between the first line receiving data and the escalation should not exceed a strictly defined time (for example, 20 minutes). Second line specialists can investigate an incident from minutes to weeks, gathering detailed data, bringing in experts, restoring the sequence of actions, and preparing recommendations for dealing with the consequences of the incident, implementing countermeasures, and raising awareness.

Second line employees should have deeper expertise. It is recommended to carry out temporary rotation of employees within the SOC: Second line specialists should work part of the time in the first line, and first line specialists should be involved in the investigation of some incidents. These measures are aimed at improving the quality of SOC work, increasing the professional level of employees and increasing their motivation. As part of these rotations or at a separate time, second-line specialists (or a separate team of experts) should improve the metrics that are used by first-line specialists in the analysis and escalation of incidents, as well as analyze atypical and anomalous activity.

The system administrator maintains SOC systems, participates in the development and deployment of new infrastructure features, configures and maintains sensors, creates custom signatures, scripts, and is responsible for automation.

Considering a large organization, such as a critical infrastructure, it is possible to use an expanded set of functions and a complete separation of roles and responsibilities. A possible organizational model for a large SOC is shown in Figure 10.

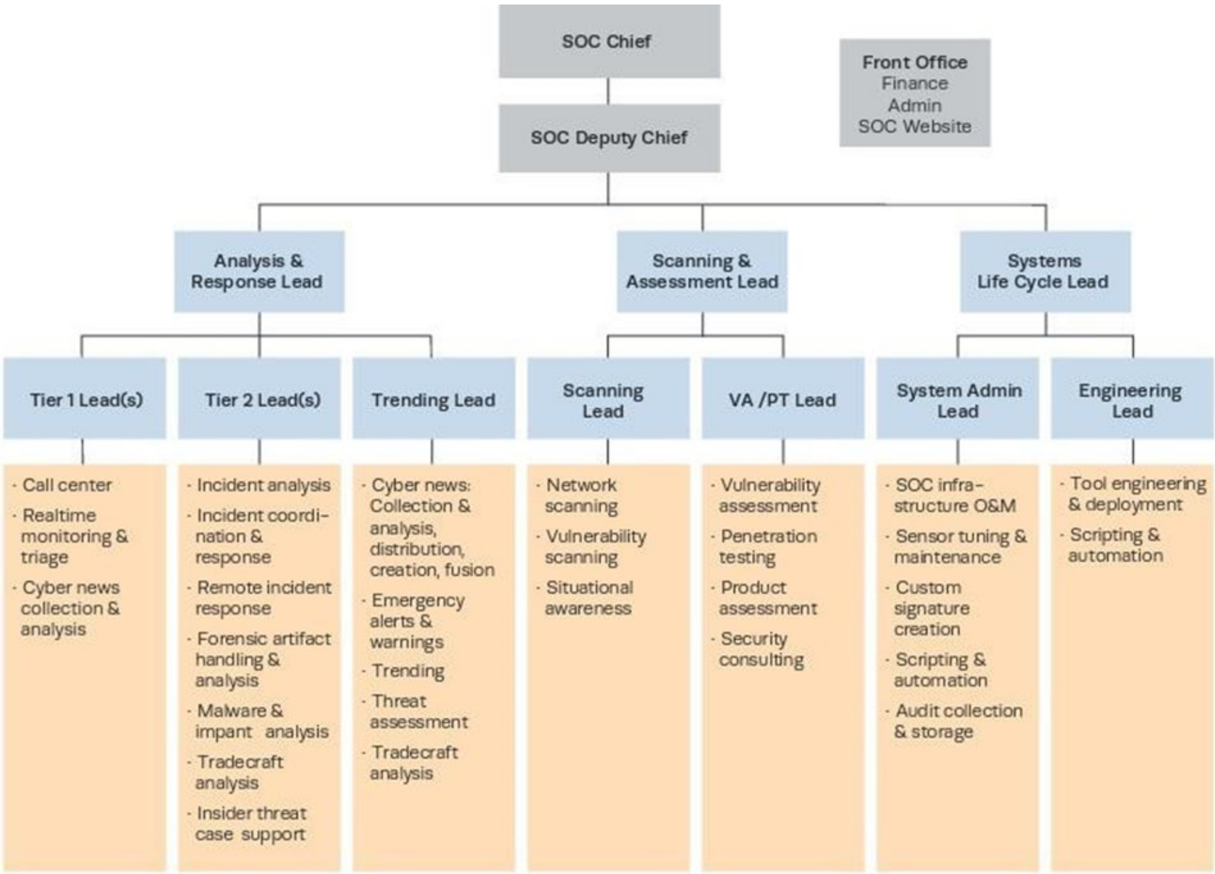


Figure 10. A large SOC role model example. Source: Carson Zimmerman

As in a small SOC system, as in a large one, it is important to ensure there is effective cross training and cross-pollination. Engineering must stay cognizant of the ops group’s main challenges and “pain points” and how to quickly leverage 90 percent solutions. Moreover, even though we may have multiple layers of management; operators in one section should not hesitate to work directly with any other part of the SOC. [15]

An important issue that often causes a lot of controversy is the mode of operation of the SOC. The ideal option is to work 24/7/365 at full capacity. Many, especially directed attacks are carried out at night. This leads to the fact that when working in 8/5 mode, a full-fledged reaction will follow only by lunch of the next business day, when analysts will clear up the blockage of data for the night (or weekend) and sort out the situation. Therefore, the staff works in 3 shifts of 24 hours. Depending on the SOC of the system, there may be a different number of personnel. If this is not a state-owned enterprise, then there should be at least 3 people in the shift: 2 employees and 1 manager. If this is a state enterprise, then from 12 to 15 people.

Step 3: Technology

With an understanding of the people and processes that an SOC system performs, it is time to look at the technologies used by the Security Control Center (SOC).

SOC must be equipped with tools to automate the IR processes. Some of the tools can be basic tools like antivirus, firewall and intrusion detection system. Others can be advanced tools such as data leak prevention, application security testing, database activity monitoring or automated vulnerability assessment tools (Lacey, 2013). At a minimum, all core security and SIEM controls should be in place to create integrated SOC functions (Lacey, 2013).

The information technology market has a wide variety of tools and ready-made systems that can help organize SOC at the physical level. It all depends on the size of the system and the invested budget. The only thing left to do is to understand the technology and determine the main elements necessary for the functioning of the SOC system. Figure 11 shows a SOC logical chart.

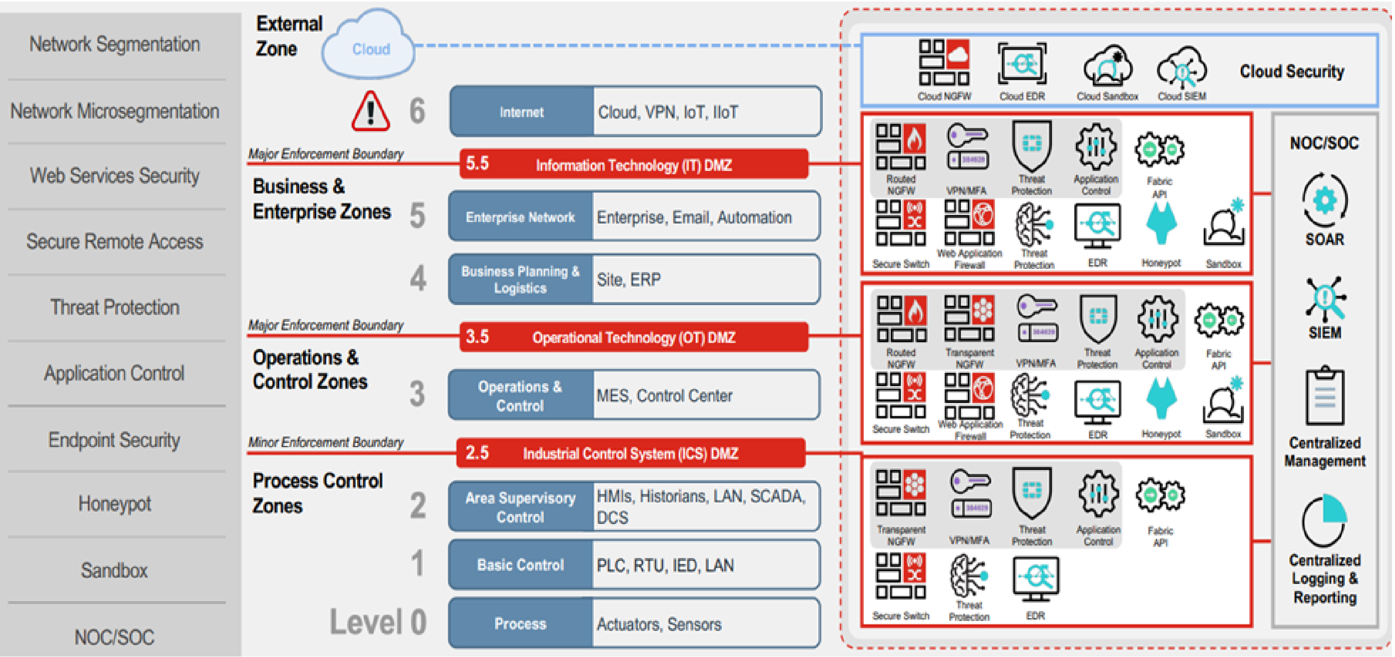


Figure 11. Modern SOC logical chart

Logically, the SOC system is divided into zones, and the zones into levels. Each DMZ zone is a separate network segment containing public services and separating them from private ones. This provides an additional layer of security on the local network, which allows minimizing damage in the event of an attack. The chart shows which technologies and tools can be used in each zone. For example, in the process control zones, can be used the following tools: Secure Switch, VPN, EDR, Fabric API, Application Controls, Threat Protection, Transparent NGFW. Each element physically (Secure Switch) or programmatically (Threat Protection, Application Control, Fabric API) detects threats, providing security, eliminating security holes, providing faster prevention and efficient operation.

The main technologies used in the creation of SOC:

1. *Network Segmentation* - is one of the most effective architectural concepts for securing OT environments. The idea is to divide the network into a number of functional segments or "zones" (which may include sub-zones or micro-segments) and make each zone accessible only to authorized devices, applications and users. The firewall defines and enforces zones, and defines channels that allow sensitive data and applications to pass from one zone to another. The architectural model of zones and channels significantly reduces the risk of intrusion. Users or devices authorized to perform certain actions in a particular zone can only function normally in that zone (Fortinet, A Security Approach for Protecting Converged IT and OT).

2. *Network Microsegmentation* - is the process of creating sub-zones at a more granular level, with fine-granular controls around individual or logically grouped assets (Fortinet, Security Strategies for Confronting Advanced Threats to OT). Such a division is clearly visible in chart 8. Four zones (Process Controls zone, Operations and Control Zone, Business and Enterprise Zone, and External Zone) and each zone is divided into several levels - subzones (Process, Basic Control, Area Supervisory Control, Operations and Control and e.t) that control certain processes.

3. *Web Services Security* - it is a standard required for the secure exchange of data within web services. The standard describes three core technologies: authentication (how to attach security tokens to identify the sender), integrity (how to sign SOAP messages to ensure integrity), and confidentiality (how to encrypt SOAP messages to ensure confidentiality).

4. *Secure Remote Access* - is a technology used to provide secure remote access to systems or applications. Use secure remote work strategies and efficient and secure technologies for remote access. For example, Virtual Private Network (VPN), Endpoint Security, Strong Password Policies, Multifactor authentication, Security training and awareness and other.

5. *Threat Protection* - is a service that detects and investigates attacks on networks and helps to respond effectively to them.

6. *Application Control* - it is a security technology that blocks or restricts the execution of unauthorized applications. Control functions depend on the goals of a particular application, but the main one is to ensure the confidentiality and security of data used and transferred between applications. Applications are divided into four groups: safe, dangerous, highly restricted and weakly restricted. Depending on this, the level of restrictions imposed is determined. For each group of applications, rules are set, according to which access to various resources (files, folders, registers, network addresses) is regulated. For example, if an application needs access to a particular resource, Application Control checks to see if it has the appropriate rights and then performs the operation according to the specified rules. Application launches are also logged. This information is used during the investigation of incidents and various checks. The functionality (power and usability) determines how effectively network administrators can implement and maintain various security policies.

7. *Endpoint Security* - detects events on user and servers end nodes also can be used for logging and detailed analysis of what is happening at the operating system level. An EDR system

can serve as an event source for a SIEM system.

8. *Honeypot* - A tool simulates a computer system with applications and data to detect various types of threats. The principle of the "trap" is very simple. Cybercriminals take it for real and hack. The data obtained during the attack helps to understand the attacker's strategy, the means used, thereby contributing to the correct distribution of information security resources.

9. *Sandbox* - it is a mechanism for the safe execution of programs. It is used to run unverified code from unknown sources and detect viruses. In fact, the code is run on an isolated station under close supervision. This is relevant when malware pauses at the start of its work. The sandbox, using behavioral analysis technologies, detects threats in files that are transmitted over the network (mail messages, downloading files from the Internet, etc.). The mechanism helps detect and prevent threats before they infiltrate a specific host.

10. *NOC/SOC* - it is an integrated management and analysis solution, with the functions of a network operations center (NOC / Network Operational Center) and a security operations center (SOC / Security Operation Center). This tool automates IT processes and threat response, assesses measurable security performance, monitors the status of SIEM elements and operations, and combines Analyzer and SIEM capabilities.

CONCLUSION

Undoubtedly, critical energy infrastructures offer increased levels of protection and security against physical threats and cyber-attacks. They apply specialized **ISO standards,** which aim at their secure operation. Of course, nothing is 100% secure so security measures should be evaluated at regular basis in order to reassess security measures, improve security measures and generally prevent. European critical energy infrastructures are adequately protected against cyber threats. However, this is not something that should be avoided, as new practical system breaches are discovered at regular basis, which is why it is useful to apply models of future threat predictions. Critical energy infrastructures data networks must be designed to ensure the security, integrity, confidentiality, and authenticity of the information provided and control mechanisms. The use of **air-gapped** network in critical energy infrastructures **must** be considered a prerequisite for their operation. Of course, there must be alternative secure networks that will be used in emergencies in combination with virtual systems, which will also be used in emergencies in combination with the retrieval of secure information from backup systems. Network devices must be from trusted manufacturers as well as for their installation must be done by reliable and trusted staff. The vulnerability assessment must be carried out throughout the critical energy infrastructures **methodically** and at regular basis in order to eliminate the possibility that even a vulnerability has been created also with the use of parameters security vulnerabilities can be discovered which until then had not been discovered.

Building a SOC is a long and costly process. It is not worth doing it in a hurry. It is necessary to determine the goals, available resources, make a plan and move consistently, solving task after task. As a result, it is possible to create for your organization the most powerful tool for combating information security incidents, a living and unique organism called SOC.

When creating or upgrading SOCs, it is necessary to take into account the problems and opportunities of previous generations of operations centers. Before making any changes, it is necessary to assess the current level of information security: this will help identify security gaps. Recall and evaluate recent incidents to make sure you have the means to detect them. Cyber-attacks should stimulate methods and means of their detection. Understanding where the vulnerabilities are will help determine what technologies are needed. Choosing the right technology will reduce the volume of signals that people have to process, enabling them to focus on problems that technology cannot solve. After all, people in SOC are of great importance.

Staff training is a very important matter in which money and hours are worth spending. Proper training of staff is what will save the critical energy infrastructures at the critical moment by taking the necessary measures that are required to be implemented in accordance with the applicable security policy. The staff are the ones who will undertake the recovery procedures after a disaster and the review of the systems, the staff must be well trained and able to deal with any event always according to their responsibilities and the training that has been done for the sector concerned. The security policy that is faithfully implemented by the critical energy infrastructures identifies the security measures and countermeasures that the staff must know and have been trained in.

Software used in critical energy infrastructures must be certified. Software from various sources should **not** be used without proper certification. Staff should have limited access to files, which include software, operating system files, sensitive files, operating files, etc. The security policy specifies exactly the level of access that staff should have according to the needs of each sector. Control mechanisms should be evaluated regularly for the purpose of evaluating the faithful implementation of security policies as well as the completeness of their operations. Backup storage processes must be secure, backup storage must be secure, virtual alternative systems must also be secure. Finally, encryption of communications, control functions, certifications, and information transmitted over the data network is a significant advantage over threats of information interception and access to control systems.

The one that needs deeper research, which is not covered in detail in this handbook, is the further research of the integrity of information, control operations, and in general the communications **between air-gapped network and non-air-gapped network**, it is worth analyzing the danger of the point of the one who **possibly** these two separate networks with some security policy manage to exchange data with each other.

To effectively counter threats, it is necessary to change tactics and methods, introduce new technologies and automate existing processes. Therefore, the creation of SOC in critical energy infrastructure will be more effective if it is created at the state level.

Bibliography

- **[1] Christos Beretas** (2018) Security and Privacy in Data Networks. (Research in Medical & Engineering Sciences , 2018). **ISSN: 2576-8816**

DOI: 10.31031/RMES.2018.05.000617

- **[2] Christos Beretas** (2016) US Cyber Strategy of 2020. (Journal of Computer Engineering & Information Technology, 2016). DOI: 10.4172/2324-9307.1000171

- **[3] Michael Coole , Jeff Corkill , Andrew Woodward , Michael Coole , Jeff Corkill , Andrew Woodward** (2012) Defence in depth, protection in depth and security in depth: A comparative analysis towards a common usage language. (SRI Security Research Institute, Edith Cowan University, Perth, Western Australia, 2012). DOI:10.4225/75/57a034ccac5cd

- **[4] Brian T. Bennett** (2017) Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel, 2nd Edition. (Wiley; 2nd edition, December 21, 2017). **ISBN: 1119237785**

- **[5] Ronald L Krutz** (2016) Industrial Automation and Control System Security Principles. (International Society of Automation; 2nd edition). **ISBN: 1937560635**

- **[6] Christos Beretas** (2020) Industrial Control Systems: The Biggest Cyber Threat (Journal of Scientific and Technical Research, 2020). **ISSN: 2574 -1241**

DOI: 10.26717/BJSTR.2020.31.005143

- **[7] Bianca Scholten** (2007) The Road to Integration: A Guide to Applying the ISA-95 Standard in Manufacturing. (ISA, March 30, 2007). **ISBN: 0979234387**

- **[8] Ashish Makwana, Jayesh kumar Pitroda** (2016) Ready Mixed Concrete Selection through Management Approach: Analytical Hierarchy Process (AHP) and Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) method. (LAP LAMBERT Academic Publishing August 19, 2016). **ISBN: 3659939668**

- **[9] Ricarda Koch, Ralph Lueftner** (2019) Communication Networks in Automation: Bus Systems, Industrial Security and Network Design. (Publicis; 1. edition 4 Dec. 2019). **ISBN: 3895784524**

- **[10] Edward J. M. Colbert, Alexander Kott** (2016) Cyber-security of SCADA and Other Industrial Control Systems. (Springer; 31 Aug. 2016). **ISBN: 3319321234**

- **[11] Clint E. Bodungen, Bryan L. Singer, Aaron Shbeeb, Stephen Hilt, Kyle Wilhoit** (2016) Hacking Exposed Industrial Control Systems. (McGraw-Hill Education Ltd; 22 July 2016). **ISBN: 1259589714**

- **[12] U.S. Department of Commerce, National Institute of Standards and Technology** (2017) Guide to Industrial Control Systems (ICS) Security. (CreateSpace Independent Publishing Platform 4 July 2017). **ISBN: 1548557781**

- **[13] Pascal Ackerman** (2017) Industrial Cybersecurity: Efficiently secure critical infrastructure systems. (Packt Publishing 18 Oct. 2017). **ISBN: 1788395158**

- **[14] Mark Roy Long** (2022) A Small Business Guide to the Security Operations Center (SOC). https://www.fool.com/the-blueprint/soc/.

- **[15] Kathryn Knerler, Ingrid Parker, Carson Zimmerman** (2022) 11 Strategies of a world-class cybersecurity operations center. (MITRE Corporation, 2022). **ISBN: 979-8-9856450-7-1**

- **[16] Joseph Muniz, Gary McIntyre, Nadhem AlFardan** (2016) Security Operation Center Building, Operation and Maintaining Your SOC. (Published by Cisco Press November 2015). **ISBN-13: 978-0-13-405201-3**

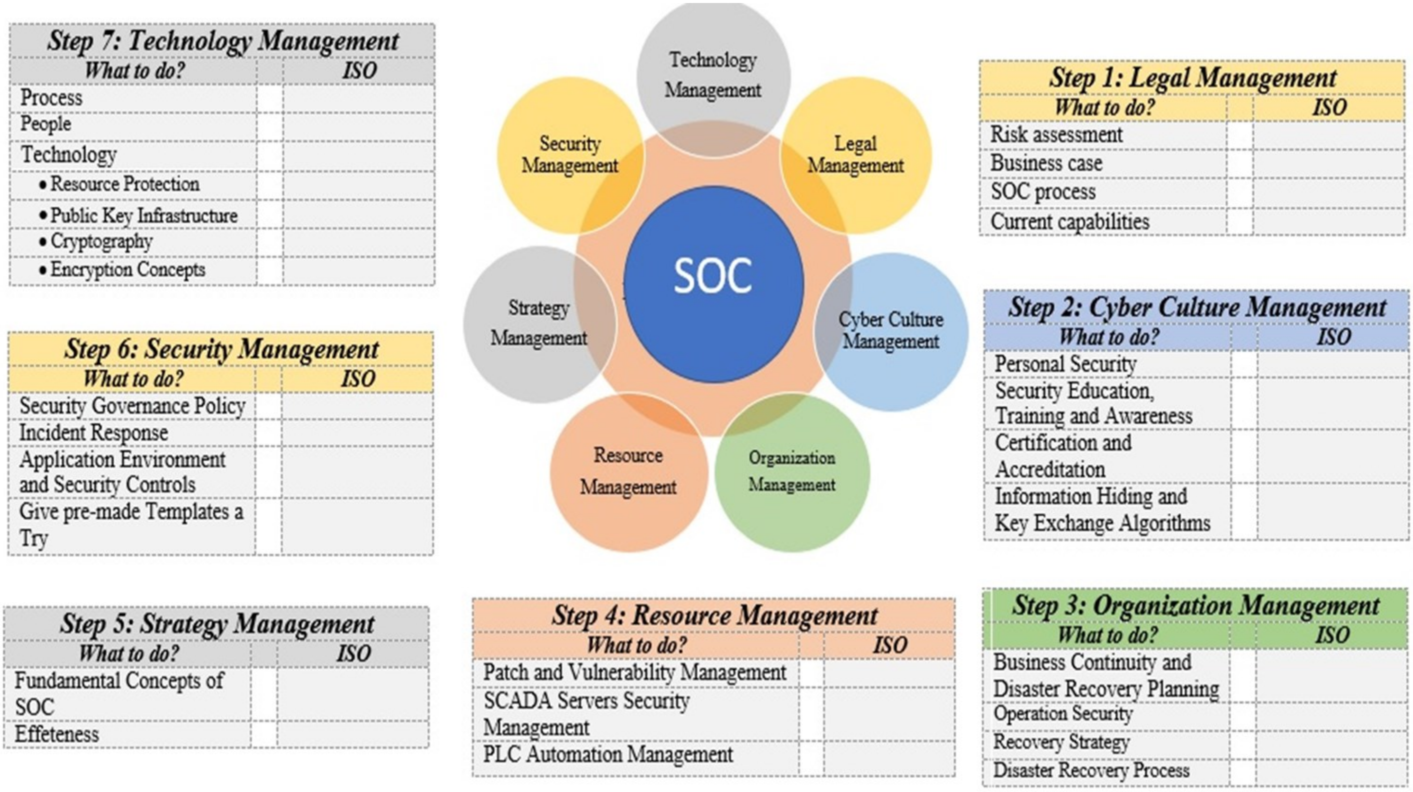
- **[17] Babu Veerappa Srinivas** (2014) Security operation center (SOC) in a utility organization.

- **[18] Joseph Muniz** (2021). The Modern Security Operations Center The People, Process, and Technology for Operating SOC Services. (Addison Wesley 2021). **ISBN-13: 978-0-13-561985-8**

- **[19] Carson Zimmerman** (2014). Ten Strategies of a World-Class Cybersecurity Operation Center. (The MITRE Corporation 2014). **ISBN: 978-0-692-243210-7**

- **[20]** https://www.trellix.com/en-us/security-awareness/operations/what-is-soc.html#overview

Annex I - Check list for determination ISO standards



Step 1: Legal Management		
What to do?		*ISO*
Risk assessment		
Business case		
SOC process		
Current capabilities		

Step 2: Cyber Culture Management		
What to do?		*ISO*
Personal Security		
Security Education, Training and Awareness		
Certification and Accreditation		
Information Hiding and Key Exchange Algorithms		

Step 3: Organization Management		
What to do?		*ISO*
Business Continuity and Disaster Recovery Planning		
Operation Security		
Recovery Strategy		
Disaster Recovery Process		

Step 4: Resource Management		
What to do?		*ISO*
Patch and Vulnerability Management		
SCADA Servers Security Management		
PLC Automation Management		

Step 5: Strategy Management		
What to do?		*ISO*
Fundamental Concepts of SOC		
Effeteness		

Step 6: Security Management		
What to do?		*ISO*
Security Governance Policy		
Incident Response		
Application Environment and Security Controls		
Give pre-made Templates a Try		

Step 7: Technology Management		
What to do?		*ISO*
Process		
People		
Technology		
• Resource Protection		
• Public Key Infrastructure		
• Cryptography		
• Encryption Concepts		

Source: made by the author

Annex II - Guidance for organization set up SOC

Item	What	Answer	Points
1	Give yourself 1 free point because you will have an incident at some point in time.		
2	Has your constituency detected an incident that had a measurable impact on the mission or came at a significant cost within the last six months?		
3	Is there a perception that your constituency faces a targeted external cyber threat beyond the normal Internet-based opportunists such as script kiddies?		
4	Does your constituency serve a high-risk or high-value business or mission and is that mission heavily dependent on IT, such as finance, healthcare, energy production, or military?		
5	Does your constituency offer IT services to directly connected third parties in a B2B, B2G, or G2G fashion?		
6	Does your constituency serve sensitive or privacy-related data to untrusted third parties through some sort of public-facing portal such as a Web application?		
7	Does your constituency retain sensitive data provided or owned by a third party, such that the constituency faces significant liability if that data is stolen or lost?		
Subtotal			
	How many thousands of hosts are in your constituency?		
	Multiply the subtotal by the number of thousands of hosts in your constituency. This is your total.		

Source: Carson Zimmerman

For questions 1–7, if the answer is "yes," give yourself one point; if not, zero points. At the second line from the bottom of the table, enter the number of thousands of hosts in your constituency. Multiply the number of thousands of hosts by the points subtotal, giving the total number of points at the very bottom. As a general guideline—and this is where different experts on SOCs may have differing opinions—we pick a rough threshold of 15. Organizations scoring well above 15 are more likely to warrant a SOC. Those that score well under 15 may be better served by an ad hoc security team model or outsourced monitoring. An organization that scores right around 15 may look to other factors such as resourcing or organizational risk tolerance. Additionally, an organization's score is a loose indicator of the size and resources its SOC should have. In other words, an organization with a score of 200 probably needs a bigger SOC than an organization with a score of 20. [19]

Annex III - SOC Types

Organizational Model	Example Organizations	Remarks
Ad Hoc Security Response	Small Businesses	No standing incident detection or response capability exists. In the event of a computer security incident, resources are gathered (usually from within the constituency) to deal with the problem, reconstitute systems, and then stand down. Results can vary widely as there is no central watch or consistent pool of expertise, and processes for incident handling are usually inadequately defined.
Security as Additional Duty	Small businesses, small colleges, or local governments	No formal SOC organization. However, SOC-like duties are part of other duties. For example, a system administrator that also looks for unusual activity in system logs. Some procedures for incident response may exist.
Distributed SOC	Small to medium-sized businesses, small to medium colleges, and local governments	Formal SOC authorities. Comprised of a decentralized pool of resources housed in various parts of the constituency. Staff may have other duties as well.
Centralized SOC	Wide range of organizations including medium to large-sized businesses, educational institutions (such as a university), or state/province/federal government agencies	Resources for security operations are consolidated under one authority and organization. SOC personnel have dedicated roles in the SOC. This model is the most frequent focus of this book, the most frequent operating model, and the simplest way to think about how most SOCs operate.
Federated SOC	Organizations with distinct operating units that function independently of one another such as businesses that have acquired other businesses but have not integrated them together	A SOC, likely centralized but could also be hierarchical, that shares a parent organization with one or more other SOCs, but generally operates independently. It may have some shared policies and authorities.
Coordinating SOC	Large businesses or government institutions	A SOC responsible for coordinating the activities of other SOCs underneath it. Focuses primarily on SA and overall incident management. Does not direct the day-to-day operations of the SOCs it coordinates.
Hierarchical SOC	Large businesses or government institutions	Similar to the Coordinating SOC structure; however, the parent organization plays a more active role. The parent organization may offer SOC services to lower-level SOCs and has greater responsibility for coordinating a wider range of SOC functions (such as engineering, CTI, malware analysis, etc.)
National SOC	Country level governments	Responsible for strengthening the cybersecurity posture of an entire nation. Creates opportunities for sharing SA of vulnerabilities, threats, and events across multiple constituencies. May orchestrate activities associated with significant cyber incidents.
Managed Security/ SOC Service Provider	Organizations of all sizes	Provides SOC services to external organizations via a business/fee-for-services type relationship

Source: Kathryn Knerler, Ingrid Parker, Carson Zimmerman

1. What is the purpose of the procedure and what policy does it align with?
2. How should the SOC be involved with this procedure?
3. How long is the SOC responsible for this procedure?
4. What other groups or outside elements impact the procedure?
5. What threat does this procedure deal with?
6. What resources are required for this procedure?
7. Are logging or reporting required for this procedure?
8. What notifications should be included within this procedure?
9. What is the notification escalation process?
10. How are notifications delivered (email, mobile, home, chat, etc.)?
11. Are there any compliance elements involved with this procedure?

(Source: Joseph Muniz. The Modern Security Operations Center The People, Process, and Technology for Operating SOC Services. 2021)

Annex IV - Capability Template

	Security As Additional Duty	Distributed SOCsSmall/Young Centralized & Federated SOCs	Large/Mature Centralized & Federated SOCs	Hierarchical SOCs	Coordinating & National SOCs
Incident Triage, Analysis, and Response					
Real-Time Alert Monitoring and Triage	B	B	A	A	N
Incident Reporting Acceptance	B	B	A	A	A
Incident Analysis and Investigation	B	B	A	A	A
Containment, Eradication, and Recovery	B	B	A	A	A
Incident Coordination	B	B	A	A	A
Forensic artifact Analysis	N	O	B	A	A
Malware Analysis	N	O	A	A	A
Fly-Away Incident Response	O	O	B	A	A
Cyber Threat Intelligence, Hunting, and Analytics					
Cyber Threat Intelligence Collection, Processing, and Fusion	O	B	A	A	O
Cyber Threat Intelligence Analysis and Production	N	O	B	A	A
Cyber Threat Intelligence Sharing and Distribution	N	O	B	A	A
Threat Hunting	O	O	A	A	O
Sensor and Analytics Tuning	B	B	A	A	O
Custom Analytics and Detection Creation	O	O	A	A	O
Data Science and Machine Learning	N	O	B	A	O
Expanded SOC Operation					
Attack Simulation and Assessments	N	O	B	A	A
Deception	N	N	O	O	O
Insider Threat	N	N	O	B	O
Vulnerability Management (if performed by the SOC)					
Asset Mapping and Composite Inventory	B	B	A	A	O
Vulnerability Scanning	B	B	A	O	O
Vulnerability Assessment	N	O	B	A	B
Vulnerability Report Intake and Analysis	B	B	B	A	A
Vulnerability Research, Discovery, and Disclosure	N	N	O	B	A
Vulnerability Patching and Mitigation	B	O	O	N	N
SOC Tools, Architecture, and Engineering					
Sensing and SOC Enclave Architecture	O	B	A	A	O
Network Security Capability Engineering and Management	O	B	A	O	O
Endpoint Security Capability Engineering and Management	B	B	A	O	N
Cloud Security Capability Engineering and Management	O	B	A	A	N
Mobile Security Capability Engineering and Management	O	O	B	O	N
Operation Technology Security Capability Engineering and Management	O	O	O	O	N
Analytic Platform Engineering and Management	O	B	A	A	A
SOC Enclave Engineering and Management	O	B	A	A	A
Custom Capability Development	N	O	B	A	A
Situation Awareness, Communications, and Training					
Situational Awareness and Communications	B	B	A	A	A
Internal Training and Education	O	B	A	A	A
External Training and Education	O	O	O	O	A
Exercises	O	O	B	A	A
Leadership and Management					
SOC Operations Management	B	B	A	A	A
Strategy, Planning, and Process Improvement	O	B	A	A	A
Continuity of Operations	O	B	B	A	A
Metrics	O	B	A	A	A

Source: Kathryn Knerler, Ingrid Parker, Carson Zimmerman

- **Basic (b):** SOCs in this category typically offer this capability/service at a basic level of performance inside the SOC.
- **Advanced (a):** SOCs in this category offer this capability/service at a more advanced, mature level of performance inside the SOC.
- **Optional (o):** SOCs in this category may or may not offer this capability or function. Their choice to do so usually has more to do with their maturity, resourcing, focus, and external requirements than necessarily their organizational model.
- **Not recommended (n):** SOCs in this category are unlikely to offer this capability or function in house. This is usually due to foundational capability and competency not being present, resources being limited, or scoping the focus to what is most appropriate for the organizational model type. [15]