Security Governance Q&A

Edoardo Ottavianelli & Matteo Piermartini

1. Describe the Von Solms's ISG model and discuss the importance of implementing the Direct, Execute and Control processes as a loop.

- Von Solms's model description
- The Von Solms's model is mainly composed of three parts, specifically Direct, Execute and Control. It's important to use them as a loop instead of a one-shot solution. Why? First of all a company/organization doesn't have a short term mission and secondly it's difficult to list all the assets and directives in just one time. The core of the Control part is the set of clauses that we use to check if we are correctly securing the assets. If not, there are some problems and so we need to report them back to the Strategic team. So after each iteration it's important to study the results of the previous one and understand how we can improve the directives in order to fully secure the assets of the organization. Moreover, even if there aren't problems, organizations change their view during time and so it's necessary to also change the list of the assets to be secured and their associate directives.

2. According to Von Solms's Information Security Governance model, describe the depth dimension and discuss how it relates to the direct-execute-control loop

- Von Solms's model Depth Dimension description
- For the Directives and Control parts it's obvious, they explain how to use the loop in a better way (ISPA and compliance clauses).
  The Risk Management part tells us what Risk management is and how the risk is defined; this is important because the ISG is based on the concept of risk management.
  The Organization part describes how a company should divide its workforce into two separate parts (Information Security Operational Management and IS Compliance M).
  This is important because there should be a clear understanding of who is responsible for the directives and the implementation of them and who is responsible for checking them.

The Awareness part tells us that the teams must be trained in order to know how to effectively implement the steps of the DEC loop.
Ultimately, Best practices support all the DEC loop telling us how ISG experts and managers solved problems during the past; it's an effective way to check if we are following some good practices.

3. Discuss the Awareness dimension of the Von Solm's model with particular emphasis on the SETA program

Why
+
Desc

Since IT security procedures must be drafted and published in such a way that they are transmitted to all users of the organization, it is essential that workers are aware of and trained on policies and procedures. All this is formalized in a program known as SETA (Information Security Education Training and Awareness) whose goal is to provide users with training on the safe way to work and raise their level of awareness of the importance of protecting IT.
Let's focus now on the three terms of SETA and see what they mean:

Significato

1. Awareness is based on what the problem is. School approach in the form of videos and posters
2. Training is based on how to solve the problem. More technical approach in the form of lectures, laboratories and workshops
3. Education is based on why I solve the problem. In this way the employee is part of the security process. Theoretical approach in the form of seminars.

CCLM

During the completion of the SETA program it makes sense to talk about the Conscious Competence Learning Model that list the stages through which the employee passes:

Steps
del
CCLM

1. Unconscious Incompetent where the subject is a person who does not realize the fact that he is a person unable to do certain things and it is important to point out that he is unable to do a specific thing
2. Conscious Incompetent where the subject is being instructed to perform their work safely

Steps del CCLM + STOP

3. Conscious Competence where the subject knows how to do their job safely. But he still has to focus on getting him to do the right things (it doesn't come naturally)
4. Unconscious Competence where the subject, through experience and practice, has acquired naturalness for everything that concerns working safely.

4. With reference to Von Solms’s ISG model, discuss the front dimension and its two core principles.

DC loop intro

This section must be considered in different dimensions relating to information security (Directives, Control, Risk Management, Organization and Awareness), at the basis of which we find the best practices, which are all standards, guidelines, practices, documents developed over years of IT security by experts. Let's take a closer look at the principles we need to remember when discussing the direct-control loop. First of all we must have clear in mind that everyone must be involved in the system and that the loop therefore involves all three company levels: strategic, tactical and operational which are made up of people who have different responsibilities and skills. The second thing to remember about it is that each level has its own actions, in particular, the strategic level takes decisions (WHAT we have to do), the tactical layer indicates how things are done (HOW we have to do it) and the operational layer applies the procedures indicated by the upper layers (WHO have to do something).

Within the direct-control loop we have two arrows: one that goes from the strategic layer to the operational layer and that progressively widens and one that proceeds in reverse and that progressively narrows. This indicates that there must be communication between high and low levels. In particular, we see that the arrow that goes from top to bottom tells us that from the highest layer the things to do are decided in broad terms and are gradually made more detailed and appropriately documented as we arrive at the layer in which they are put in practice (Direct part). On the contrary, the arrow that proceeds towards the top, becomes gradually thinner and indicates that the reports produced by the operational level are very detailed and rich, while the organization's board receives only stringent considerations to see if the policies from them they are working properly or not and eventually make other decisions (They do not care if 3424 viruses or 213 malware have been detected, they want to know if things are going well and if it is safe to connect to the internet, if I have economic losses etc). Let's go into even more detail about the direct-control loop:

IN PROSA DA
CHATGPT

- Direct part of the loop

1. Strategic layer = Here the assets, their relevance and their required level of protection are identified.
INPUT: The inputs can be external (legal obligations such as GDPR, etc.) or internal (strategic vision, competitiveness, market objectives, etc.).
OUTPUT: The output of this level is a set of directives that indicate what is expected to be done regarding the protection of assets.

2. Tactical layer =
INPUT: As input you have the directives of the strategic layer
OUTPUT: The directives are then extended into a set of policies, standards and procedures.

3. Operational layer =
INPUT: As input we have the policies, standards and procedures dictated by the tactical layer.
OUTPUT: The policies of the tactical layer are then expanded into administrative guidelines and procedures accompanied by technical measurements. These are then actually implemented and managed.

- Control part of the loop

Since it is possible to manage only the things that we can measure, this concept of measurability must be ensured at the heart of all directives, policies and standards (defined in the direct part of the loop). As we have seen, one of the metrics we can use is the risk associated with something.

1. Operational layer =

→ IN PROSA DA CHATGPT

INPUT: Measurements related to data extracted from a series of entities such as sensors, IDS, IPS, syslog files, etc.
OUTPUT: Produce detailed technical reports containing all useful information based on the extracted data.

2. Tactical layer =>
INPUT: Having taken the operational layer report, it is necessary to decide if the policies, standards and procedures are suitable for protecting the assets (for example if I have a policy that tells me that employees cannot connect to the corporate network with their devices, they will check how many abnormal connections have occurred).
OUTPUT: Also in this case a report is produced, but much poorer in terms of details than the one of lower layer (tactical management report) indicating the levels of compliance.

3. Strategic layer =

INPUT: Having taken the tactical management report as input, the board must understand how things are going within the organization, study the underlying causes of the observed phenomena and try to understand if there are problems that can lead to economic losses for the organization (Situational Awareness).

OUTPUT: As the output of this layer there is a report that reflects compliance with the most important directives including risk considerations (Are expectations met?).

5. Discuss the role, the importance, design and realization of Standard and Best Practices in the context of an Information Security Governance system.

COS'È E QUALI

We know that the best practices are at the base of the vertical stacks of the Von Solms's Model. They consist of a set of documents, standards, guidelines developed over years of IT security by thousands of well-known experts (ISM Information Security Manager). These help us protect the right resource in the right way. Each ISM must therefore answer these two questions:
- How do I know which are the right assets?

~~I don't have a clear answer to this question. I can only speculate what are the fundamental assets for a given organization.~~

- Assuming you understand what the right assets are. How do I know if I'm protecting them well? I follow the best practices. Don't waste your time finding a solution to a known problem, but adopt a solution that has already been effective in the past! There are obviously different standards: ISO 27000 family, COBIT, NIST, CSC etc.
  - Brief introduction about NIST CSF
  - Brief introduction about ISO 27k family

6. Describe the structure of the NIST CSF and explain how it can be used to plan investment related to cyber security.

In 2014, the President of the United States of America commissioned NIST (National Institute of Standards and Technology) to implement a framework for managing cybersecurity risks. Then the NIST-CSF was born. An important point is that it should be adopted on a voluntary basis, i.e. it is not required by law because there are already mandatory certifications, safety laws that companies must abide by, but this standard is more a collection of general and flexible guidelines that can be good for everyone. The basic idea is not to refer to expensive and complicated solutions so that, for better or worse, the catchment area of organizations that make use of good cybersecurity practices expands (everything in about 60 pages). The second basic idea is to manage IT risks together with all the others in the organization's Risk Management process.

In the first version we wanted to focus on improving cybersecurity for critical infrastructures but with the most recent revisions (2018) we wanted to extend the standard to all organizations whose work is based on the use of technology: Internet of Things, Information Technology, Industrial Control Systems, Cyber-Physical Systems.

Furthermore, the framework has been developed to be technologically neutral, that is, we focus on solving problems regardless of the specific technological environment on which the standard is actually used.

Then another feature is given by the fact that NIST-CSF is the result of years and years of study on cybersecurity and the document is full of references to other standards, other best practices, etc. (This makes it very comprehensive). Finally, another important point is the common

taxonomy for organizing the lifetime of security. In this taxonomy they have organized functions, categories and controls, creating a homogeneous structure that makes the standard suitable for different applications. One of these is self-assessment of one's own security position. ("How far am I from my goal?" Or "How different is my position from that of another organization?" And this is a question that can arise when I am signing a contract with a partner and see if its standards are compatible with mine).
Therefore, NIST-CSF supports security assessment, planning and monitoring activities.

Core Part:
It makes up more than a third of the entire document. Tree based structure. It might look like a checklist but it's not. In fact, it is more a collection of recommendations that we should think about applying within our organization. Since it is not a checklist it cannot be used to assess compliance (part of the framework, in fact, may not be used in your organization due to the generality of the document). The core consists of 4 elements:
1. Functions: Used to organize cybersecurity at a high level. There are essentially 5 functions:
(a) Identify: Here we focus on what the problems may be. It includes all aspects related to developing understanding about cybersecurity. In particular, in this section, we focus on the identification of critical assets, people and processes (Remember, you don't have to protect just the infrastructures).
(b) Protect: Here we focus on the mechanisms that must be adopted to implement security procedures.
What are the actions to be performed in advance to minimize security problems.
(c) Detect: Real-time aspects. I try to understand what is happening as the forwards are always one step
ahead of me and therefore I try to detect everything that is wrong from the point of view of security. (Monitoring and similar activities)
(d) Respond: How I respond to certain problems I detect. It is the part of the framework that is activated when I detect something and I have to interrupt the attack phase of an opponent.

(e) Recover: What do I do if the attack is successful? Mechanisms are suggested to be adopted in order to recover from an accident and return to normal operations (before the attack took place). If you read from top to bottom we can somehow see the lifetime of the security
2. Categories: are particular aspects that contribute to the definition of a single function.
3. Sub-categories: subdivide a certain category into particular cases.
4. Informative References: which represent references to existing standards and best practices.

Implementation tiers:
It covers aspects orthogonal to the core. The criteria for evaluating the type of security approach of an organization are included here. These criteria are not based on the number of mechanisms I implement, but on the degree of maturity of the security process. In fact, I can implement a few mechanisms in a very structured way and implement many in a completely unstructured way. There are usually 4 implementation tiers and range from "partial" to "adaptive", that is, from the least rigorous to the more structured. Normally,
when I enter a tier, I CANNOT use this parameter to compare my security level with that of another organization. Since positioning myself in these levels, as mentioned, only tells me "how rigorous and structured I am in my approach to security", it does not tell me anything about the quality of the security process. Ideally, we always start from tier 1 and should move towards the higher tiers, but this must all be commensurate with the context of the organization I manage.
N.B. Advancement to a higher tier is recommended if it is convenient from an economic point of view.

Profiles:
With the profile, I combine the functions, categories and sub-categories (of the core) with the business requirements, with the risk tolerance and the resources of the organization. It is very useful for describing the current security status but also the target security status, in a sense. Furthermore, seen from this perspective, it allows us to carry out a gap analysis, that is, it allows me to calculate the efforts needed to move

from a certain safety position (in which I find myself) to an ideal one (target security posture).
However, remember that NIST-CSF, to date, does not provide you with any example of profiles and therefore there are no reference points: I have to create the reference profiles on my own!

Due to the fact that we can perform an internal security assessment, it's possible to understand our cybersecurity posture, which are the primary and secondary assets in the organization, the defenses in place in order to secure them, which are the goals and the risks those assets are subject to. This can help an organization to have a clear view of its cybersec position and how far it is from the objective and so in understanding the investments (not only financial, but also effort, technologies, people...) to be done in order to reach the goals.

7. Comparison between ISO 27001 and NIST SP 800-53

In general:
They both have references to other standards and therefore somehow talk about the same stuff, albeit with a different level of depth. We reiterate, however, that every FISMA standard is system-oriented, that is, they tell you "how to be done" (wrt Implementation Details), in ISO you do not find anything of the kind. Additionally, NIST and all FISMA standards certify the IT part of the organization, while ISO is for information security management system certification. One point in common is the work to create the two standards which took years of effort.

NIST 800-53 is part of a series of special publications called the NIST-SP 800 series. These are strongly detailed documents and full of very specific aspects or in any case restricted to particular topics. NIST 800-53 focuses on the controls that federal agencies must apply to ensure a certain level of security and privacy (463 pages). It is simply a collection of checks that organizations check for self-assessment and also provides a selection method for checks.
The controls are organized into 18 families, each of which collects some within it, connected in some way in that family precisely. Each control has the following structure:

- Control ⇒ which contains the activity / action to be performed in your system
- Supplemental guidance ⇒ It gives us additional information on the implementation that may or may not be mandatory, depending on the level of security to be achieved.
- Control enhancements ⇒ They allow you to improve the implementation of the control (references to enhancements are present in the priority and baseline allocation, for the MOD and HIGH sections it is often intended to reduce the impact of the controls)
- References ⇒ They are references to documents, laws, regulations, standards and best practices that give us a reason why the control itself exists.
- Priority and baseline allocation ⇒ How relevant is the control with reference to the baseline and its impact. It can recommend actions to be taken depending on the level of impact LOW, MOD(erate) and HIGH.

Baselines ⇒ The aim is to facilitate the choice of controls to be adopted as the standard has many. Even if we wanted to use them all, we should still list them according to a criterion

Prioritization ⇒ We can say that the baseline are the controls with the highest level of priority which is linked to the level of impact.

Limits of NIST 800-53:
1. All proposed approaches focus on the US federal corporate environment. The document is very complex and aimed mainly at the operational level. No manager would be able to make decisions by reading this alone.
2. Does it make sense to take this certification outside the US? In Italy, for example, we could hardly obtain this certification, because we could avoid following one or more checks that are superfluous or not required here. However, it can be considered an excellent starting point for the implementation of controls.

ISO 27001 is a standard that guarantees information security and data protection within organizations and defines the requirements for establishing, implementing, maintaining and improving an ISMS.
Unlike ISO 27002, this is a standard for obtaining a certification and therefore is much more rigorous and specific and details what an organization must have or do to be compliant. For the check comes the auditor who checks if all the checks are followed (There is no flexibility).

Limits of ISO 27k:
1. Many of the standards require certification and this means costs (for the implementation of new or retrofitted security processes, for the creation of particular divisions within the company context,) and this for small and medium-sized enterprises is a consistent sacrifice.
2. Typically these standards do not provide for a prioritization of controls and each of these is mandatory to receive certification.
3. It is your choice to apply for certification (NIST is mandatory in the USA instead).
4. Again, this class of documents is NOT aimed at management (although it is less technical than NIST).

8. Establish the truthfulness of the following sentences
It is possible to get a ISO/IEC 27001 certification
It is possible to get a ISO/IEC 27002 certification
It is possible to get a certification in compliance with the NIST CSF
NIST CSF can be used for internal assessment and auditing
The certification NIST 800-53 is not mandatory in USA
Provide a brief motivation of your answers

- It is possible to get a ISO/IEC 27001 certification: True
  It is a standard that guarantees information security and data protection within organizations and defines the requirements for establishing, implementing, maintaining and improving an ISMS. Unlike ISO 27002, this is a standard for obtaining a certification and therefore is much more rigorous and specific and details what an organization must have or do to be compliant. For the check comes the auditor who checks if all the checks are followed (There is no flexibility).
- It is possible to get a ISO/IEC 27002 certification: False

It is a document that contains best practices and is structured as a sort of tree: it is made up of 14 security provisions (clauses), each of which contains one or more security categories.
ISO 27002 containing guidelines and it does not force anyone to follow them all and therefore proves to be much more flexible

- It is possible to get a certification in compliance with the NIST CSF: False
  An important point of NIST CSF is that it should be adopted on a voluntary basis i.e. it is not required by law because there are already mandatory certifications, safety laws that companies must comply with, but this standard is more a collection of general and flexible guidelines than they can fit everyone. The basic idea is not to refer to expensive and complicated solutions so that, for better or worse, the catchment area of organizations that make use of good cybersecurity practices expands.
- NIST CSF can be used for internal assessment and auditing: True
  An important point is common taxonomy for organizing the lifetime of the security. In this taxonomy they have organized functions, categories and controls, creating a homogeneous structure that makes the standard suitable for different applications. One of these is self-assessment of one's own security position. ("How far am I from my goal?" Or "How different is my position from that of another organization?" And this is a question that can arise when I am signing a contract with a partner and see if its standards are compatible with my partners). Hence, NIST-CF supports security assessment, planning and monitoring activities.
- The certification NIST 800-53 is not mandatory in USA: False

9. Describe the main options available in the risk treatment phase and discuss (if they exist) some guidelines for their selection according to the possible different combinations of likelihood and impact (e.g., risk treatment option x is better in case of likelihood y and impact z because…)

The risk treatment is the set of activities aiming to identify and select means for risk mitigation and reduction.
In principle, we should seek to treat all risks that are unacceptable, but in the end this is a question of cost and benefit, no matter the risk level:

- if a low risk is very cheap to eliminate, we might do so even if the risk in principle is acceptable.
- if the cost of treating a very high risk is unbearable there may be no other option than to accept it.

The risk treatment activity, therefore, should involve both the identification and the analysis of treatments

The analysis should take into account that some treatments can create new risks, and that some groups of treatments can reduce the isolated effect of each other.

Once the risks, sources, costs have been identified and the risk matrix has been elaborated. Based on the scale used, I will have high, medium or low level risks and I will be able to do two things: accept the risk as it is or mitigate it. In particular:

- Risk Reduction: I want to reduce, for a certain risk, the probability of its occurrence and / or the consequences associated with it.
- Risk Retention: I accept the risk because it has a low probability or because the consequences are easily amortized.
- Risk Avoidance: In this case I want to remove the causes of the risk. I am not reducing probabilities or consequences, but removing the risk at its root, making sure that the risk cannot materialize in any way. It is usually used in combination with risk reduction.
- Risk Sharing: I absorb some of the risk and typically sign a contract with an insurance company that shares the risk with me.

10. Describe the main steps of a risk management process and discuss peculiarities of handling cyber risks.

The main steps of a risk management process are:

1. Scope, context and criteria:
   Here we need to identify and describe the context of the risk assessment process.

   We must focus on the environment in which we are working, distinguishing external and internal elements:
   a. Internal context: structure of the organization, processes, dependence between the elements of the process, etc.

b. External context: In some way we focus on the environment in which the organization to be analyzed is located.

Let's now see what are the activities to be carried out during the definition of the context:

a. Identifies the assessment target ⇒ usually the part of the system subject to risk analysis.
b. Scope of the assessment ⇒ I decide what I want to include in the analysis and what I want to exclude, and why
c. Focus of the assessment ⇒ the perspective from which I want to conduct the assessment.

2. Risk assessment: In turn divided into
    a. Risk identification: In particular we will identify and describe (document) the risks and possible sources of risk ⇒ Everything that can go wrong and why they can go wrong

       For every real risk we have three essential characteristics:
       (a) Asset ⇒ Element that will be impacted by the risk
       (b) Vulnerability ⇒ What can be exploited by the attacker to damage the asset
       (c) Threat ⇒ The way in which the exploit is conducted from a source of threat
       If even one of these features is missing, then we are not facing a risk.

    b. Risk analysis: At this point we can estimate the level of risk identified. In particular, the level of risk derives from the combination of probability and consequences:
        i. Estimation of probability ⇒ Identifies the probability that the accident I am analyzing will materialize. I can do it in any way, statistically, through market analysis etc. It is not an easy task.
        ii. Estimation of the consequences ⇒ The consequences are connected only to the asset. Normally they are then linked to loss of money, due to the payment of fines,

        loss of market value of the company, etc. The estimation in this case is simpler and is based on historical data of similar accidents or historical analyzes.

    c. Risk evaluation:
        i. Risk consolidation: Once we have identified probabilities and consequences, we make the product and calculate the value for that risk.
        ii. Evaluation of risk: We will then put that value within the risk matrix and see what there is to do with that risk, that is, if we can accept it or have to treat it in some way. However, before moving on to any treatment, we must make some considerations. In fact, we must consolidate the results of the risk analysis by focusing on the values about which we are most uncertain.
        iii. Risk aggregation: Then we aggregate the risks, i.e. I can combine two risks that have similar characteristics from the point of view of the assets they afflict or from the point of view of the sources of threat, treating them as a single risk. Obviously, in this case, I gain from the treatment point of view because if I inhibit the source of threat for one, I resolve it for the others as well.
        iv. Risk grouping: group risks that have elements in common
    d. Risk Treatment: Once the risks, sources, costs have been identified and the risk matrix has been elaborated. Depending on the scale used, I will have risks with a high, medium or low level and can do two things: accept the risk as it is or mitigate it.

The peculiarities of handling cyber risks are more or less the same for the normal risk management process:

1. Communication and consultation: One of our tasks here was to identify all stakeholders. The problem with cyberspace is that since cyberspace can be extended to the whole world, we could potentially have stakeholders scattered everywhere.
2. Risk Management:

a. Scope, context and criteria: For the external context, let's analyze the relationships between customers and providers, the amount of attack and regulations such as the GDPR. For the internal context, the attack surface and the possible services that I am exhibiting are determined.

b. Risk Assessment: Risks can be distinguished from malicious and non malicious. We can build a “Risk model” for both kinds of risks.

   i. Risk identification of cyber-risks malicious:

      1. Malicious threat source identification: who is the attacker, the motives of the attack, the ability of the adversary, ect.
      2. Malicious threat identification: The origin of the threat can be internal or external. For this we should document all the procedures leading to the attack. We could also use directory such as NIST, ISO, OWASP and MITRE.
      3. Malicious vulnerability identification: We must focus on the attack surface, such as lack of awareness, ect.
      4. Malicious incident identification: Some of the vulnerabilities clearly have different effects than others, so if some exploits affect all 3 security properties of an IT system (Availability, Confidentiality, Integrity) others will only affect two or one.

   ii. Risk identification of cyber-risk non malicious:

      1. Malicious incident identification: Typically they are the result of accidental events whose source is normally given by an external condition.
      2. Malicious vulnerability identification: In this case the vulnerabilities are mainly due to some bugs in the system (unintentional).
      3. Malicious threat identification: Again, we don't have a known methodology, but ISO 27005 can come back to help.

4. Malicious threat source identification: We can always use the tables offered by ISO / NIST etc. but we could also provide a generic classification of all possible accidental causes: environmental conditions, weather conditions, errors in system design, etc.

c. Risk Analysis: We must divide the factors for likelihood and consequences in malicious and non. We could use techniques such as threat modeling, attack paths, attack trees, etc.

d. Risk Evaluation: Here we have four phases:
   i. Consolidation of risk
   ii. Evaluation of risk
   iii. Risk aggregation: 2 incidents afflicts the same asset OR 1 incident afflicts 2 assets
   iv. Risk grouping: 2 incidents benefits from the same patch/fix

e. Risk Treatment: Reduction, Retention, Avoidance, Sharing.

11. Talk about OWASP Risk Rating Methodology

This approach is based on the two-factor risk model: Risk = likelihood x consequences. And in all it has 6 phases:

1. Risk identification:

We collect information on threat agents, which would basically be the attackers, the attack that must be conducted, the exploited vulnerability and finally the impact on the business process once the attack is successful.

2. Factors for estimating likelihood:

There are a number of factors that can help us estimate likelihood, organized into two distinct sets.

(a) Factors for threat agents; thanks to which we want to calculate the probability that an attack will be successful if performed by a particular threat agent. To identify this likelihood we use the following factors that describe the attacker: skill, motive, opportunity, size.

(b) Factors for vulnerability: with these factors we calculate the likelihood of a vulnerability based on certain characteristics: Ease of Discovery, Ease of Exploit, Awareness and Intrusion Detection.

3. Factors for estimating the consequences:
When considering the consequences of an attack it is important to realize that there are two types of impact:
(a) Technical consequences: affecting applications and data mainly. The technical impact is divided into: Loss of Confidentiality, Loss of Integrity, Loss of Availability and Loss of Accountability.
(b) Consequences on the business: it is the most important and concerns the economic and legal fabric of the attacked organization. The impact on the business is divided into: Financial Damage, Reputation Damage, Non-Compliance, Privacy Violation.
4. Determine the severity of the risk:
Here we put together the estimates of likelihood and consequences to calculate the severity of the risk. We generally rely only on technical impact if the business impact estimate is not good. Typically the mapping between numerical value and risk level is like this:
0-3 Low / 3-6 Medium / 6-9 High
However, we can conduct this analysis by following two approaches:
- Informal method: In some cases it is not wrong to consider only the summary values of some factors and simply deduce the most important aspects of the risk analysis through some considerations ⇒ Identify and focus only on the key factors
- Repeatable method: If, on the other hand, it is necessary to make the assessments repeatable, we must resort to a more rigorous process of calculating the risk factors ⇒ The concept of uncertainty is always valid in this case. These estimates are intended as an aid to the assessor to arrive at a reasonable result. Very often, however, automatic tools are used to calculate these factors.
5. Decide what to fix:
Once the overall risk level has been established, the risks to be fixed must be prioritized. The first general rule is: higher level risks are mitigated first ⇒ don't be stingy! And don't focus on the little things that cost little first
The second general rule is: not all risk fixes are smart ⇒ If a mitigation costs me 100,000 euros to prevent 2000 euros of stolen data a year, it's never worth it!
6. Customize the risk rating model:

Having a customizable framework for a company is essential for it to use it. There are several ways to develop a custom model and among them stand out:

- Add factors:

The assessor can decide whether to choose different factors to represent what is important for the company. (For example, a military application may have an added factor linked to the loss of human life)

- Custom options
- Review the factors:

Earlier we assumed that all factors are equally important, but during the customization process, we can make the factors most important to our business matter more in some way and then I'll have to do a weighted average in likelihood calculation. and consequences.

In light of the above, let's now see what are the pros and cons of this risk rating methodology:

PROS:

- Structured in a few steps
- Easy to apply
- Supported by an open-source tool

CONS:

- Allows only a rough risk analysis
- It doesn't help much during the mitigating phase

12. With reference to threat modeling, describe the asset-centric, the attack-centric and the software centric approaches highlighting for each of them advantages and disadvantages**.**

Asset-centric approach

To be used when we want to focus on the consequences of risks affecting the assets, business process side. Useful if we have critical assets and we want to protect them in the best way.

The focus of the analysis is on the set of assets and on everything that can go wrong in the role of the defender, who must identify what is important for the organization, and what can go wrong in the role of the attacker, who must identify the assets it wants to target. Operationally speaking, we will follow these 3 phases:

1. Make a list of your assets and their vulnerabilities. Then, for each of those present, identify how an attacker can exploit the vulnerabilities.
2. Bind assets to the IT infrastructure in order to identify how an attack can enter the system and compromise the assets themselves.
3. Redesign the system until you can tell a story about them.

To support this model we can use STRIDE or an attacker-center brainstorming.

Attacker-centric approach
Difficult to list all the threat sources.
To be used when I am trying to improve awareness and / or want to provide a remediation plan. Here it is imperative to think like a striker. I start from all the possible attack techniques, I analyze what can be the possible set of attackers who can use them, and then I try to understand how to apply what has been said in the system. To support this methodology, we can refer to some repositories, such as CAPEC for example. Typically, this technique allows us to identify threats that are related to human vulnerabilities.
To be used when I interface with the human side of the organization.

Software-centric approach
Useful to find the clear differences between software we want and bugs and unrequired functionalities (thanks also to DFD or UML).
To be used when we want to check if we are subject to a specific threat. I start from the idea that the software I have is not what I ideally have in my head. In the latter case, in fact, the software contains only the features required during the design. In the ideal case the software I have exactly coincides with the required features. However in the real case I will have that the software I have is a mix of required features, unsolicited features and bugs. Obviously bugs and unsolicited functions are vulnerabilities, so you have to find them all and fix them, where possible. Ideally, we need to conduct software centric analysis during the design period, as this approach is indicated during software design. In reality, however, when designing software, security is never given importance (especially if the system is in production).

How should I model the software?
We need to create a diagram that allows me to see the software and its interactions with external entities:

1. Via Flow chart ⇒ Although not widely used during threat modeling, this allows us to observe the flow of data well, however it does not allow us to see how the system / software is composed.
2. Via Data flow diagram - DFD ⇒ It allows us to proceed with a top-down approach. Iterate over the system components. This method focuses on the inputs and thus on the data types exchanged between the components. ⇒ High level view of the information system.
3. Through Universal Model Language - UML ⇒ Represents the system from a different perspective.

13. Describe what is an attack graph and its three main usage scenarios.

By attack graph we mean a graphical representation that identifies all the possible ways that an attacker can follow to enter inside the system. It tries to correlate a series of vulnerabilities that are found in the different hosts on the network and then tries to understand if they can be exploited in sequence, based on the privileges that the attacker obtains at the time of the intrusion.
Typically an attack graph is composed of:
1. Nodes, which represent the host / device on the network and its privileges
2. Edges, which represent a possible vulnerability that I can exploit from a certain (source) node to obtain some kind of privilege on another (target) node. The vulnerability obviously lies on the target node.
To produce an attack graph we must therefore know some information about the system: vulnerabilities and reachability conditions, for example firewall rules between subnets.

For a more detailed graph, we can use the following rules:
- All the nodes, except the junction ones, must contain the following information:

    1. IP address of the node
    2. CPE ID which is a standard method for the identification and description of the application

3. Name of the application which is the user-friendly version of the CPE

- In purple nodes (privilege nodes) there is a category that indicates the software system connected to the privilege. For example: file access privileges, memory access privileges and so on.
- In the yellow node (vulnerability node) there is the CVE ID that uniquely identifies the vulnerability we are trying to exploit

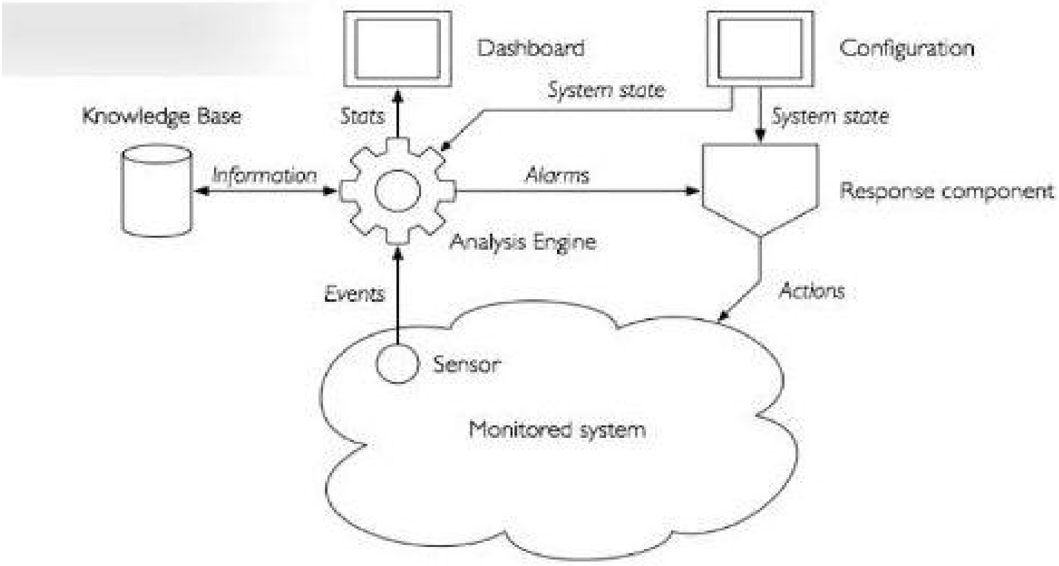
The three main usage scenarios are:
1. Calculation of network security metrics:
We will use it, in our case, to support the risk analysis. We will therefore use an algorithm that creates the attack graph for me and also measures the risk associated with it. In this case, all we can do is identify the source and target in the attack path system and then calculate the risk of the specific situation. I do not use a specific threat model because I am not eliciting a particular threat but in this case the threats are implicit and are represented by all the attack patterns that you can calculate taking into account the vulnerabilities and their possible exploits. So I can calculate the risk based on the threat agent, the different attack paths (I can exclude for example those with too long lengths)

2. Support network hardening:
The idea is to calculate the attack graph in order to identify the best mitigation method. In this case, the mitigation actions are expressed in terms of vulnerability patches (like I remove the specific set of vulnerabilities) or I can think in terms of reachability (I change the configurations in order to reduce the risks: I change the firewall rules, or opening / closing the doors of the devices, or I can decide whether to turn off or turn on a certain service on a machine. But I can also think of improving the Intrusion Detection Filters (include some monitors in specific areas of the network).

3. Near real-time security analysis:
It uses attack paths as possible paths that an attacker can follow to perform an exploit and monitors, via IDS alert, whether these attack paths were actually followed or not. If I see that an attacker is following a path, then I cut the link of the path in order to interrupt his offensive.

14. Describe the structure of Intrusion Detection System discussed during the lecture

The most common elements among the different existing IDS are the following:



We have:

- Monitored system = the infrastructure that I want to protect and monitor to detect suspicious activity.
- Sensors = acquires information from the system and sends it to the analysis engine. Work in event-based mode.
- Analysis engine = collects all the events received from the sensors, analyzes them and, during this phase, acquires information from a possible knowledge base. Compare info from the knowledge base and compare it to system events.
- Knowledge base = This can be internal or external to the IDS, and contains information relating to typical attacks or system behavior.
- Dashboard = The high-level information is then displayed here in the dashboard and made available to analysts, who must interpret the behaviors in the system and, where necessary, issue an alarm.
- Response component = If our defense includes a response component to a malicious event (prevention component ⇒ typical of IPS - Intrusion Prevention Systems), this collects the warning linked to the alarm, interprets it and acts in some way in the

system to promptly block the threat (for example, DoS attack detected, IPS blocks connections with suspicious IPs).
- Configuration = Obviously the answers to be implemented in the system are defined in advance by the security operator.

15. Describe the taxonomy of Intrusion Detection System putting particular emphasis on the different techniques that can be used to perform the analysis

There is a large variety of IDS and therefore it makes sense to provide a classification of the most common ones. We can group them all on the basis of 5 macro-categories that correspond to peculiar characteristics:

1. Information Source:
    a. Host Based: The idea is to monitor events involving a specific host. Typically we collect information inside the machine and its interfaces, however we will not explicitly consider the interactions, but more the flows it generates. In particular, we will analyze log files (at the access level, OS, applications, etc.), network traffic, processes performed, file access and configuration changes. The typical techniques used in these cases by the IDS are: code analysis, sandbox executions, traffic analysis, filesystem monitoring, log analysis.
    Typically this approach is used for the company's most sensitive hosts, such as a server. Or when I want to analyze data exchanged in an encrypted communication.
    CONS:
        - Complex configuration
        - Negative impact on performance

    b. Network Based: The idea is to monitor traffic on a network segment. Not only the traffic to the interfaces but also that in transit between hosts: the way in which information is exchanged, the frequency, the type of data, the protocols, etc. Information can be analyzed at different levels of the ISO / OSI stack: application layer (HTTP, SMTP, DNS etc.), Transport / Network layer (IP, TCP, UDP, ICMP), Data-link layer (MAC, ARP).

How can it be used?
- inline, that is, it allows the passage of traffic inside it (I place the sensors on the gateways or the fire-walls), moreover, as for an IPS, I can block the traffic in a timely manner and therefore also the attacks;
- passive, here I simply duplicate the traffic (mirroring) and redirect it to the IDS, which will analyze it.

Typically, network based IDS work in stealth mode, i.e. they do not associate traffic with IPs, but only keep track of the interfaces and for this reason they are very resistant to attacks, however, they consume a lot of resources because they need to analyze the traffic in transit. on it or even after being mirrored. Although it is very expensive, it is in most cases transparent, i.e. it does not interfere in any way with the flow of data. Obviously, as already seen, IDSs of this type are useless in encrypted channels.

c. Application Logs: It only monitors specific applications, typically related to data: database management system, content management system, accounting system, etc. In this case, the IDS has access to information that host-based and network-based IDS cannot access, simply because they look at the system logs. Either I configure my host-based IDS to read the log files or I have to rely on IDS of the type under consideration. Of course, it can also track session information. However, this type of IDS is difficult to set up because I don't know in detail what is the granularity of the logs taken into consideration.
d. Sensors Alert: Basically they are sources of information that come from software sensors that provide data collected from the environment. Typically in this case the IDS is hierarchical-based or graph-based topology.
e. Wireless Networks: Here the problem is given by the diversity of communications. In fact, the communications are largely of the broadcast type ⇒ there is no routing in the network and this implies that the communication is based on a sort of quorum (gossip-based approach) and therefore this

absence of middleboxes (routers, which convey on traffic) means that I do not know where to put the sensors (this is also due to the fact that a wireless network has no well-defined boundaries ⇒ sensors in motion, since the topology of the network is dynamic). We only have devices and applications ⇒´ it is difficult to separate the malicious traffic from the legitimate one.

Finally, another CONS, for this type of IDS´ is that, since system monitoring is a process that stresses resources, and that wireless devices are often battery-powered or in any case have little energy available, there is a risk of consuming the latter. in a very short time.

2. Analysis Strategy:
    - a. Anomaly Detection: In this case, the focus is on identifying the anomaly with respect to normal behaviors. Anything that does not fall under normal behavior is marked as an attack, so here my model is the absence of anomalies. We can classify these IDS into several subclasses:
        - i. Programmed system: The system is configured with a fixed model of normal behavior (default deny, carefully elaborated; descriptive statistics, normal behavior is described through a statistical model)
        - ii. Self-learning system: The system builds the normal behavior model by itself, there is no a priori one (Non-time series, stochastic model that does not consider the temporal correlation between events; time series, temporal correlation between events)
        - iii. Rule-based methods: It characterizes the normal behavior of users, networks, and hosts as a set of rules. When a set of rules is violated, then an alarm is triggered for a suspected attack.
        - iv. Statistical methods: Some system variables are monitored which are the basis of its behavior. After that, their changes are tracked and based on the average values of these changes it is possible to see if they exceed certain thresholds.

    v. Distance based methods: We try to characterize the normal behavior through a vector and what we want to do is to measure the geometric distance between this vector and the one that represents the observations. We then provide a measure of the deviation.
    vi. Profiling methods: In this case we want to create a profile of the normal execution of the system and after that I use this profile to conduct my analysis. The matching takes place exactly as in the previous cases. The advantage is that the profile is more general than the process model.

b. Misuse Detection: Strategy based on knowledge of previous attacks. We have the attack model and what we are going to do is define the incorrect behavior or the signature of the attack. The IDS will ignore all normal behaviors and will only look for those that match the collected signatures. Everything works fine when I have the attack paths and I can immediately recognize the incorrect behavior, but if I had to have even a small deviation from the signature, this analysis strategy would not be useful.
   In this case I have four subclasses of IDS:
    1. Signature-based: SNORT is an example. I check the attack fingerprints in the database and compare the behaviors I find in the system to see if there is a matching. They work, almost like an antivirus. However, as we have seen, I am unable to detect new attack paths or slightly modified attack paths. Remember that the signature DB must always be updated !!!
    2. Rule-based: It performs the matching by evaluating the "if ... then" conditions. For each type of attack I have a set of rules that should be checked and depending on the ones I have I can classify the set of events I am observing in one or more attack classes.
    3. State transition analysis: In this case the idea is to build a finite state machine that represents the evolution of the attack. Try to match the events I am observing on

the automata. On each automaton it will have particular states that will allow us to classify the events in a specific class. Here the problem is the way in which events are received and analyzed (if I miss even one event I can arrive on an automaton that classifies my event as normal when it is not).

4. Machine learning-based: Each event is a set of attributes with a certain value and so is each attack. The model (recurrent neural networks, decision tree, SVM, etc.) tries to learn the attribute pattern that marks an attack on me. This approach is also very effective for attack variants.

3. Time Aspects (Prediction):
   a. Online tools: In the online IDS category, the data is analyzed online for the note, that is, they take a stream of data as input, analyze it at runtime. Useful for detecting threats early and reacting promptly. Obviously the resources required are many.
   b. Offline tools: In this category of IDS the data is analyzed after being collected. In this case the performances are absolutely not a problem, however I lose in timeliness of detection and promptness of reaction.
4. Architecture:
   a. Centralized: A centralized architecture IDS has the advantage that the calculations are performed at one point in the system and this simplifies configuration and management. But on the other hand or a single point of failure and I also have scalability problems.
   b. Distributed & Heterogeneous: A distributed architecture IDS does not have the problem represented by the single point of failure and also certainly will not have scalability problems. However, I compensate for the configuration and management problems, especially because I have to face headaches such as the synchronization of the different analyzers, of the data processing methods and of the reaction methods.
5. Response:

a. IDS: The IDS, normally, when they detect suspicious activity, they raise an alarm.
b. IPS: Given their nature, in addition to sounding an alarm, they try to implement non-destructive measures to combat the attack. For example, they can patch or change ACLs and firewall rules.

16. Describe the main phases of the Incident Management Process putting particular emphasis on the organizational structures and professional profiles involved

Preparation

Incident response methodologies typically emphasize preparation establishing an incident response capability to timely respond to incidents, but preventing incidents by ensuring that systems, networks, and applications are sufficiently secure is also paramount. Preparation is composed of two main activities:

• Preparing to handle Incidents: In order to handle incidents efficiently and effectively there is the need to define:

- Communication and Facilities, that is, the mechanisms by which incidents are reported, and structures/facilities as contact Information, Incident reporting mechanism, Issue tracking system, etc.
- Analysis Hardware and Software tools: Digital Forensics workstation, Laptops, Removable media, etc.
- Incident Analysis Resources: Documentation, cryptographic hashes, list of critical assets.
- Incident Mitigation Software: Clean OS and application for restoration.

Many incident response teams create an emergency kit which is a portable case that contains materials that may be needed during an investigation. The jump kit should always be ready to use and includes: a laptop, loaded with appropriate software (e.g., packet sniffer, digital forensics), backup devices, blank media, and basic networking equipment and cables. Since the purpose of having a jump kit is to facilitate quicker responses, the team should avoid borrowing items from the jump kit.

• Preventing Incident: Keeping the number of incidents that occur low is crucial because the higher the number of incidents within the system, the greater the likelihood that the response team will not be able to resolve all problems promptly. Therefore some fundamental activities must be put in place to prevent most incidents and among these we find:

- Risk assessment
- Host security
- Network security
- Malware prevention
- User awareness and training

Detection and Analysis

Developing a step-by-step guide to managing incidents is not the smartest possible solution as an incident can occur in many different ways, so it would be better to manage incidents starting from the identification of their common attack vectors: external/removable media, attrition (e.g. brute force attacks), web etc. For this reason, it is crucial to be able to detect and classify incidents by looking at two important “signs”:

• Precursors are those signs that warn us that an incident can happen in the future.

• Indicators are those signs that an incident may have occurred or may be occurring now.

Sources of Precursors and Indicators: IDPSs, SIEMs (Security Information and Event Management), Antivirus and antispam software, File Integrity Checking software, Third party monitoring services, Operating system, service and application logs, Network device logs, Network Flows, Publicly Available Information, Information on new vulnerabilities and exploits, People from within the organization, People from other organizations

Incident Analysis

Incident detection and analysis is affected by several factors such as accuracy (False Positive), a huge amount of events/alerts to analyze, indicators may follow from different root causes (not necessarily related to an incident) and many incidents are not associated with clear symptoms. The best thing to do is build a team of highly experienced and proficient staff members who can analyze the precursors and indicators effectively and efficiently and take appropriate actions. For this reason, there are 10 recommendations for Incident Analysis:

1. Profile networks and systems
2. Understand normal behaviors
3. Create a log retention policy
4. Perform event correlation
5. Keep all host clocks synchronized
6. Maintain and use a knowledge base of information
7. Use internet search engines for research
8. Run packet sniffers to collect additional data
9. Filter the data
10. Seek assistance from others

In case of suspect of an incident running, it is fundamental to start to record facts related to the possible incident:

- Timeline
- Supporting tools should be adopted
- Preserving integrity and confidentiality of collected data is important

Incident Prioritization

In the end, incident handling should be prioritized during triage, typically, based on the main factors such as:

- Functional Impact of the Incident
- Information Impact of the Incident
- Recoverability from the Incident

The classification and prioritization of incidents are essential for an organization, because resources are optimized if these are limited.

Incident Notification

Incidents should be notified to the appropriate individuals so that all who need to be involved in the response will play their roles. This should be supported through notification lists and procedures that should be specified in security policies and through multiple communication strategies which should be defined as fault-tolerant.

Choosing a Containment Strategy

This is one of the most important procedures as it allows us to stop the incident, and therefore stop the waste of resources and block the growth of damage. In some cases, it serves to gain time to come up with a repair strategy. Since this is a decision-making process, developing a predetermined strategy is a great idea. In fact, organizations should define acceptable risks in dealing with incidents and develop strategies accordingly. Note that Containment Strategies are incident dependent. Criteria for determining the appropriate strategy include:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability
- Time and resources needed to implement the strategy
- Effectiveness of the strategy
- Duration of the solution

Evidence Gathering and Handling

Gathering evidence during an incident has two main purpose:

- to resolve the incident
- for legal proceedings

In such cases, it is important to clearly document how all evidence (including compromised systems) has been preserved.

Identifying the Attacking Hosts

Identifying an attacking host can be a time-consuming and futile process that can prevent a team from achieving its primary goal i.e. minimizing the business impact. The most commonly performed activities for attacking host identification are:

- Validating the attacking host’s IP address.
- Researching the attacking host through search engines.
- Using incident databases.
- Monitoring possible attacker communication channels.

Eradication and Recovery

Eradication may be necessary to eliminate components of the incident, disable breached user accounts and identify and mitigate all vulnerabilities that were exploited. In recovery, administrators restore systems to normal operation, ensure that systems are functioning normally, and remediate vulnerabilities to prevent similar incidents. The procedures involved in this last phase may include: restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords and tightening network perimeter security.

Lessons Learned

This is one of the often omitted parts of the whole procedure, but one of the most important, namely the one that concerns learning and improvement. Questions to be answered include:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

17. In the context of incident management activities, describe and discuss the incident handling life cycle

The incident management process is divided into 6 phases, the central part of the process is however the Incident handling, which can be divided into a cycle:

- Detection and reporting ⇒ I detect the incident in some way and report it to the security analyst.
- Triage ⇒ The analyst tries to identify its severity (prioritization), then tries to understand if the incident can be ignored or must be managed in some way.

- Analysis ⇒ Analyzes the evolution of the accident.
- Incident response ⇒ Plan an adequate response to the incident under analysis.

These 4 phases of the incident handling cycle can be seen as an integral part of an even more general cycle:
- Preparation ⇒ Typically includes all activities aimed at preventing the accident and preparing the structure to react (detect and react activities).
- Incident handling loop ⇒ The preparation activities give life to the incident handling loop therefore: detection, triage, analysis and incident response. Note that after responding to the incident, I continue to observe the environment to review the situation and assess whether the response given was effective in resolving the incident or I have only mitigated it and must continue to resolve it in some way. And I continue with the loop until the incident is resolved.
- Post-incident analysis ⇒ Once the dangerous situation is over, I start with the post-incident analysis. This analysis will provide me with feedback on the causes of the accident, the techniques used to bring down the accident, the way in which we managed the accident, so to speak. Based on what is reported in the analysis, I can decide whether to change things in the system (long-term countermeasures) or I can change the steps related to the preparation phase.

In some way, therefore, the incident handling life cycle is a particular instance of the direct-control loop that aims to improve the general process of incident handling and therefore incident management.

18. Describe what is a SOC, its main responsibilities and design principles. Finally, discuss the main differences and common points between activities carried out by a SOC and by a CERT.

SOC is a centralized security organization that assists companies in identifying, managing and recovering from a distributed attack that aims precisely at security. Therefore, the ultimate goal of SOC is to improve the security of an organization by detecting and responding to threats and attacks before they impact the company business. The main services offered by the SOC are:
- Log management
- Security monitor

- Security incident management
- Vulnerability assessment
- Security analysis from SIEM's data
- Threat intelligence

Using a SOC is extremely important in the presence of critical or sensitive data or processes, not to mention that, in general, the growing trend of companies that are no longer able to keep up with security management (bottleneck due to outsourcing , or contracts to external companies). SOCs provide technical and monitoring capabilities.

SOC security operations triad:
SOC is at the heart of 3 elements:

1. People
2. Processes
3. Technologies

Remember that when you want to create an efficient SOC that delivers effective services, you cannot ignore these 3 elements, thus selecting the right people (training for tool / awareness and software, experience in the field, internal training to update one's skills), right technologies (Endpoint, Netflow, Network monitoring, Threat intelligence, Forensics, Incident / detection and management) and the right processes (preparation, identification, containment, eradication, recovery and Lesson learned - the phases present in the incident handling life cycle).

The organization of the SOC is:
The SOC has 3 levels, above which there is the manager, who is responsible for all SOC activity. There is a hierarchical structure as you can see: the strategic layer is that of the SOC manager, the tactical layer is included in layer 2 and layer 3, and finally, layer 1 is equivalent to the operational layer. Let's see them now in more detail:

- Layer 1 ⇒ Made up of analysts who acquire data from the environment, aggregate them and provide input for the next layer.
- Layer 2 ⇒ Made up of incident responders, highly specialized personnel with expertise in the field of security analysis. Their purpose is to correlate the information coming from several sources, to identify which are the response actions that can be implemented. Finally, their output will become the input for the upper layer.

- Layer 3 ⇒ Made up of hunters, grouped by service (network, intel threat, malware, endpoint). Their output will go to the SOC manager which will close the loop.

The relationship between SOC and CERT:
SOC and CERT have a complementary perspective in the support they give to organizations regarding incident analysis and rejection. Although these have one point in common which is the incident management process. All SOC activities provide the organization with a solution completely dedicated to it (Incident Prevention). They also provide, for event management, monitoring and analysis collection services and finally support the organization in incident management. If we saw the services provided by the CERT, we would have to deal with Pre-incident information, where the CERT itself collects information from internal and external sources but in this case it is not the result of a detailed analysis tailored to the client, but rather a sort of correlation of data between organizations to identify common problems, vulnerabilities and trends., this correlation will then be used for specific CERTs. After that we find the incident management, in this case, how much the CERT is actively involved depends on what is decided with the clients, there is still direct communication between the two entities. Finally we find the post-incident in which the CERT collects information on the incident which, once again, will not be used for that specific client, but to increase the overall data and made available to all clients, in order to update trends, attack patterns etc.