

*A proactive business Cyber Security Operations Center*

## **An Agile SOC Requires People's Effort**

**Renato Kuiper**

**Sandra Kagie (editor)**

**Kelvin Rorive**

**Charlotte Rugers**

**André Smulders**

**Ben van Zuijlen**

**Rob van Os**

Over the past few years many organisations have availed themselves of a Security Operations Center (SOC). Mostly, these organisations were prompted by stricter legislation and regulations (compliance driven) and acted in order to detect (potential) threats at an early stage. Within a traditional SOC, SIEM (Security Information and Event Management) has a central position, which makes a traditional SOC particularly reactive. As soon as a problem is detected, it is reported and action is being taken. However, rapid changes in the world around us and especially in the world of cyber security, require a proactive SOC. What is needed to develop from a traditional, responsive SOC (r-SOC) into a modern proactive SOC (p-SOC)? What will a contemporary p-SOC look like, prepared for the future?

*Page*

<b>2</b>	<b>MANAGEMENT SUMMARY</b>
<b>4</b>	<b>PROBLEM DEFINITION</b>
<b>5</b>	<b>AMBITIONS AND OBJECTIVES OF A MODERN SOC</b>
<b>7</b>	<b>ORGANISATIONAL STRUCTURE OF A SOC</b>
<b>18</b>	<b>SOC MATURITY</b>
<b>20</b>	<b>TRENDS &amp; DEVELOPMENTS</b>
<b>22</b>	<b>REFLECTION</b>
<b>23</b>	<b>THE WAY FORWARD</b>
<b>25/26</b>	<b>APPENDIX 1: BIBLIOGRAPHY APPENDIX 2: PARTICIPANTS</b>

## AN AGILE SOC REQUIRES PEOPLE'S EFFORT

### MANAGEMENT SUMMARY

In a traditional Security Operations Center (SOC) SIEM (Security Information & Event Management) has a central position, which makes a traditional SOC particularly reactive. However, rapid changes in the world around us and especially in the world of cyber security, require a proactive SOC.

We believe that many organisations, and especially those within the organisation who are responsible for a SOC, wonder what is needed to transition from a traditional responsive SOC (r-SOC) into a modern proactive SOC (p-SOC).

For us the answer is relatively simple: the right people. A modern and agile SOC will be predominantly centred on people's effort, as in the end it is and always will be a human decision to act upon an alarm. Only a human being can assess the broader context of an alarm, supported by technology.

#### Focus is essential

When establishing goals and ambitions of a modern SOC it is important to realise that it is impossible to do everything within a SOC. Therefore, focus on determination of your Incident and Response capabilities are essential.

There is no 'one size fits all' solution. The choice of an goal depends completely on the organisation's ambition and risk profile. Characteristic of a modern p-SOC is that they themselves take the initiative and make it a priority agenda item. For example, as a SOC, actively start the search for new threats based on threat hunting. Take the lead and show the business, especially their decision-makers, what a p-SOC can do for their organisation. This way, there is a shift of focus from reacting to detected threats to searching for unknown threats and deviations (anomaly detection). Apart from the shift from reactive to proactive, you see another transition within p-SOC, the shift from familiar to unknown (from rules to anomalies).

#### The right people

A modern p-SOC is, by its very nature, dynamic. The degree of agility in an ever-changing environment essentially brings out the power of such a SOC. It is this factor of agility that is conclusive in selecting the right people in a SOC.

Matching the right people to specific capabilities is crucial within a SOC-organisation. To promote a smooth communication between SOC and the business, it might be a good idea to appoint mutual ambassadors: Some personnel in the SOC get a role in the business and some business people get a role in the SOC, to create mutual awareness and support. In choosing the right people it is very important to keep in mind that it is not a matter of quantity, but of quality. As soon as the SOC has succeeded to bring together the right people, the next step is to retain these people. However, do not be surprised if these people leave SOC after a period of five years or so, looking for new challenges, as for some capabilities working for SOC may become routine. To maintain these employees at least for a period of five years, they should be offered challenges again and again, such as a conjugation of recurring activities of monitoring & response, in attack stimulation & hunting

threats. This way, the likelihood of retaining key personnel for a longer period of time, is greatly increased.

### **Influence of Big Data**

It is a matter of course that technical devices from a r-SOC, such as SIEM or log information from applications or security devices, such as firewalls, Intrusion Detection System (IDS) Data Loss Prevention (DPL) and so on, are still present in a p-SOC.

Seeing the ever-growing amount of data (Big Data) and threats that SOC's are confronted with, a further automation of the work load for detecting, analysing and dealing with incidents is necessary. Techniques such as 'Machine Learning' (ML), 'Artificial Intelligence' (AI) and 'Deep Learning' (DL) may be considered. In any case, it is no solution to contract more employees. It is obvious that the amount of data will keep on growing and it is a dead end to for ever expand a SOC-team. However, Big Data asks for specific new specialists and techniques in the field of data science, for complementation of an agile and modern SOC-team.

### **On the way to a tactical SOC**

It may be concluded that within a modern p-SOC human beings are essential, as opposed to a traditional r-SOC. A modern p-SOC no longer is a piling-up of technical solutions and a SOC 2017 can no longer be compared to a SIEM.

Eventually, the human factor is decisive for the success of a modern p-SOC.

A success that in the end is determined by the potential to be able to adapt to a fast-changing society in the outside world. Yet, p-SOC is no end in itself. SOC's will continue to develop into t-SOC's, tactical SOC's, that combine agility and people's effort as the key focus. Such a t-SOC proceeds towards a proactive and pre-detecting scope combined with radically automated response and will be supported by a hybrid team of members who put in combined expertise on infrastructure, applications, security, Big Data and data science for the benefit of their business.

## 1. THE PROBLEM STATEMENT OF THIS EXPERT BRIEF

What does a modern SOC that is well-prepared for the future with a special focus on human potential look like?

In this expert brief, several experts have integrated their visions and experiences so as to reach a common advice on how to organise a modern p-SOC that can face up to existing and new threats.

These experts have chosen to put human beings at the heart. In spite of technology it is the human factor within a SOC that is critical to its success. Indeed, in the end it is a human being who decides to respond to an alarm, whereby the same human being, though supported by technical devices, judges the broader context of the alarm.



**Figure 1: Originators of the SOC Expert Brief.**

*LTR: André Smulders, Kelvin Rorive, Charlotte Rugers, Renato Kuiper, Rob van Os, Ben van Zijlen.*

## 2. AMBITIONS AND OBJECTIVES OF A MODERN SOC

In general, ambitions and objectives of a modern p-SOC are twofold:

1. To get an insight into Situational Awareness.
2. Provide Incident & Response More focussed on business interest.

Situational Awareness (SA) deals with insight in the threats facing an organisation. Such threats can vary greatly: a data leakage, failing to comply to new laws and regulations, the Internet of Things (IoT), a Distributed Denial of Service (DDoS), an Advanced Persistent Threat (APT) attack, Bring your Own Device (BYOD), blind self-reliance and so on. SA (Situational Awareness) requires to be aware of risk factors and to gain knowledge through measuring and then to assess if anything needs to be done and if so, what needs to be done.

SA goes beyond Risk Management (the strategy) and Security Incident Management (the operation and organisation). SA unites Risk Management and Incident Management and in this way is the backbone of a SOC. SA offers a clear insight, not only in what to do to cope with threats (your capabilities), but also in the ability of your organisation to remain functional. To gain an integral and central insight in the organisation by constantly combining various sources of information can only be achieved by means of a SOC. More so, because in an ever-changing world there is an abundance of information, new threats pop up all the time, new laws and regulations are being published and there are ongoing changes in the internal organisation.

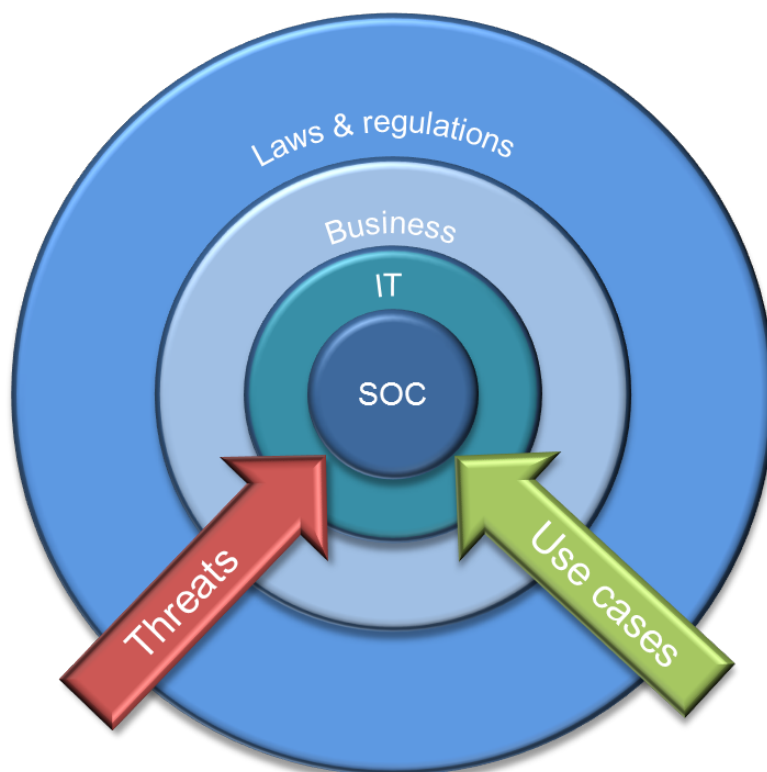


Figure 2: Position of a SOC in a continuously changing environment (Rob van Os).

Insight in SA is all-important to be able to really support primary objectives and operational processes when taking risk-based and cost-effective decisions.

When determining objectives and ambitions, it is important to understand that there is a limit to what can be done within a SOC. Therefore, it is essential to clearly define incident and Response capabilities. Consult stake holders: what are their expectations? Fine-tune ambitions. Identify what capabilities are essential to continuity of the business and develop these very capabilities or acquire them. A choice in favour of a hybrid solution is also possible: a combination of internal and external knowledge and skills.

There is no 'one size fits all' as regards the choice of objectives in a SOC, as this is completely dependent on level of ambition and risk profile of the organisation.

At the moment, a shift in level of ambition towards a p-SOC can be seen. It often was the case that no action was taken in an r-SOC, waiting for policy-makers to take a decision. Now a p-SOC more often takes the initiative itself and places spearheads on the agenda.

Communication is key here. Guide the business as well as the policy-makers and show them what a SOC can mean for their organisation.

Thus, the focus shifts from reacting to familiar threats to reacting to unfamiliar threats and deviations (anomaly detection). Apart from the transition from responsive to proactive, a transition from routine to unfamiliar takes place within a p-SOC (from rules to anomalies).

Nb. According to experts, a purely compliance-oriented SOC nowadays offers hardly any added value to organisations. Moreover, it does not show a modern level of ambition that is characterized by adapting to changes from outside (threats, business, IT and legislation). Indeed, the essence of a p-SOC is to respond to such changes again and again and by doing so to contribute to the continuity of the business.

To determine the level of ambition is closely connected with the mandate that is given to a SOC. To what extent can be required of a stakeholder or the business that they take the necessary actions after the SOC has detected a problem? A mandate roughly has three levels:

1. No mandate. SOC acts purely advisory. Advice need not be followed by CIOs, CISOs, CEOs or system owners.
  2. Shared mandate. SOC can make recommendations. These recommendations will be assessed. The SOC has a say, but not the final say.
  3. Full mandate. SOC can require actions without approval or support from above.
- (Source: Ten strategies of a World-Class Cybersecurity Operations Center. P. 17.)*

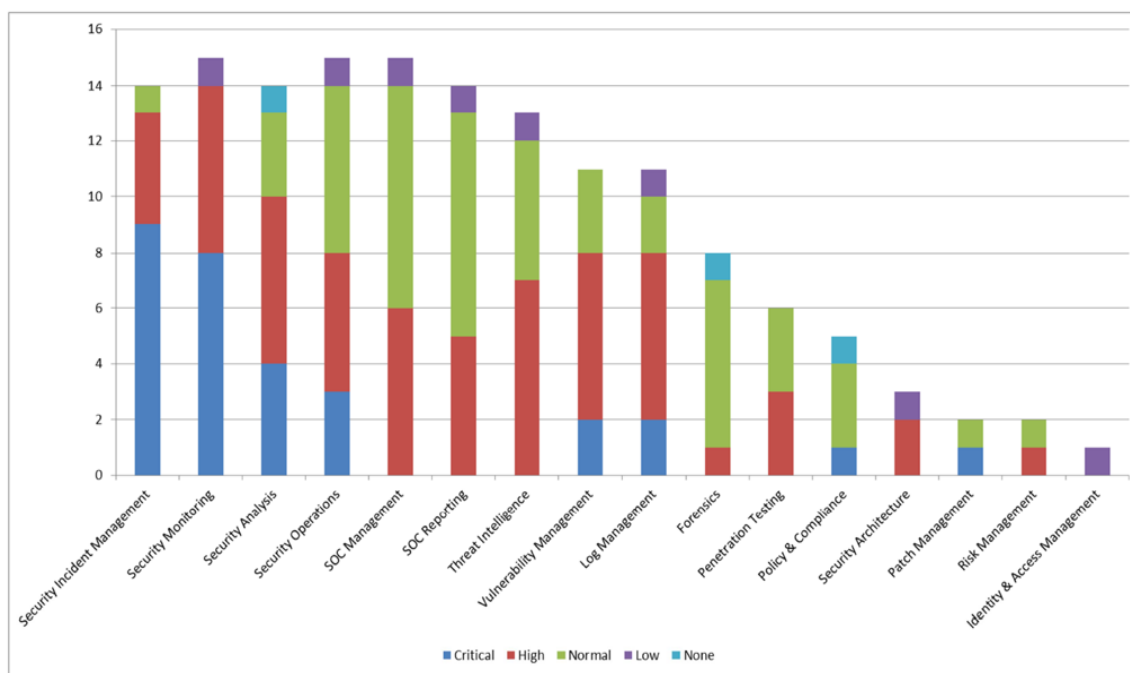
### **“Give a SOC the mandate to be able to do its work properly”**

The organisation of a SOC is based on level of ambition in combination with the mandate that has been granted and involves five pillars: capabilities, organisational structure, people, processes and technology. These five pillars will be explored in the next chapters.

### 3. ORGANISATIONAL STRUCTURE OF A SOC

#### 3.1 Capabilities

As mentioned before, it depends on the level of ambition what capabilities are being pursued. The bar graph below offers an overview of the range of capabilities to be aimed at in a SOC. Needless to repeat that focus is essential.



**Figure 3: ‘SOC-processes in use’ offers an overview of possible capabilities that can be focused on (source: Rob van Os, SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers).**

The columns in figure 3 indicate the relevance of SOC-processes in operation. Their relevance has been marked in the colours of blue, red, green, violet and light-blue. Blue denotes critical (should always be present), red is very important, green is deemed to be present in regular circumstances, whereas violet is regarded as seldom present and light-blue, finally, is considered not present.

*Nb. Relevance has been determined based on a survey of 16 participants, the number of participants who have indicated to provide this service is represented in the Y-axis.*

According to standards by the National Institute of Standards and Technology (NIST – [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)) capabilities of a SOC can be divided into various phases and accompanying main processes:

- Phase: Identify – Service: Threat Intelligence.
- Phase: Protect – Service: Vulnerability Management / Penetration Testing.
- Phase: Detect – Services: Security Monitoring, Security Analysis and Log Management.
- Phase: Respond – Services: Security Incident Management.
- Phase: Recover – Services: Recovery after a security incident, Back-up & Restore

These phases can be represented as follows:

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Source: Cybersecurity Framework 1.0

**Figure 4: Capabilities of a SOC according to the standards of the National Institute of Standards and Technology (Source: NIST – [www.nist.gov/cyberframawork](http://www.nist.gov/cyberframawork))**

Those in charge at a SOC decide what services in a SOC are relevant, dependent on stakeholders’ wishes, legal and regulatory framework and means available. On this basis decide the relevant factors within your own SOC and focus on them. The final responsibility will always be with the business and cannot be shifted to a SOC.

**“Make choices within a SOC. Focussing and Prioritising are essential for success.”**

The list of possible services is enormous. For instance, see *Table 1. SOC Capabilities – Ten Strategies of a World-Class Cybersecurity Operations Center p. 19-24*. Bear in mind that no single SOC will be able to unite all these capabilities.



### 3.2 Organisation of a SOC

A SOC can be positioned in another organisation in various ways that are decisive for the style of governance. Besides, the role of a SOC influences governance. If a SOC has been outsourced, the model will be more formal as regards to agreements, compared to the position of an intern SOC that works on its own. A SOC that functions as an in-company service provider has more agility and can respond faster to impending changes that form threats. Maturity, accountability as regards efficiency and finance are aspects that are of importance in governance.

Within the organisational structure of a SOC, people are all-important. They ultimately determine knowledge, skills and experience within a SOC. If no one is available for specific capabilities within a SOC, then a solution should be found: either by providing education within the SOC, or by hiring external staff. Hybrid staffing is becoming a trend at the moment.

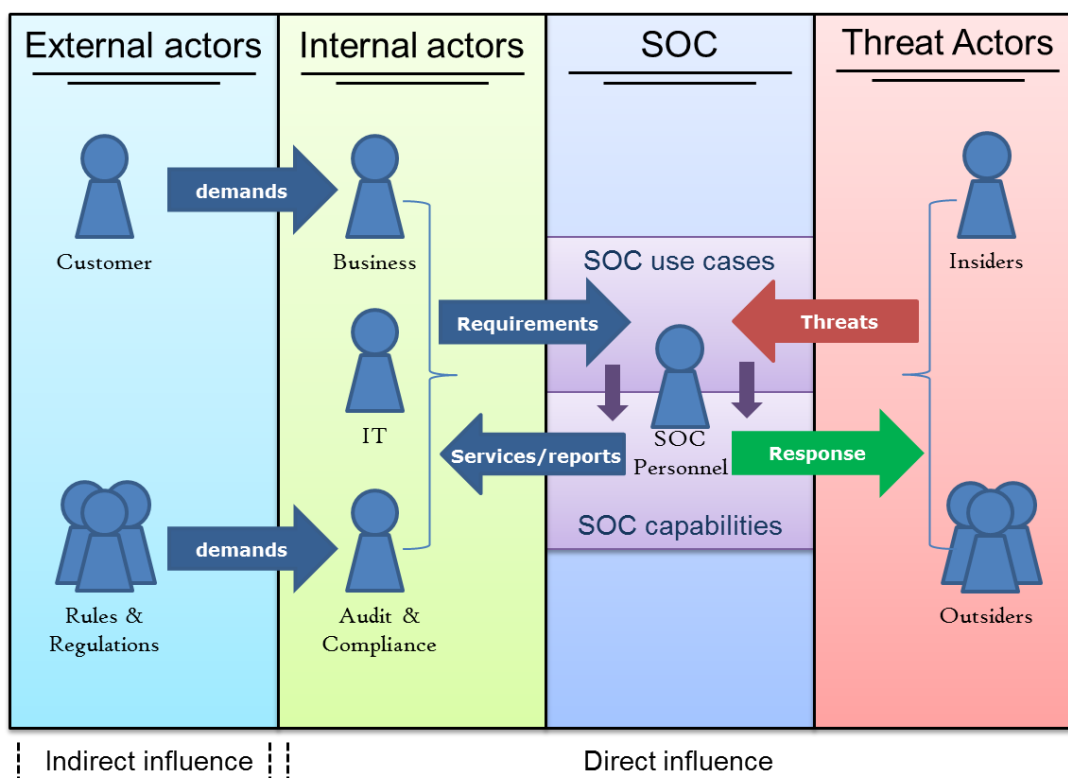
#### **“Make use of hybrid staffing within a SOC.”**

A modern p-SOC is dynamic par excellence. Indeed, in an ever-changing environment the degree of agility is key to the power of a SOC. It is this factor of agility that counts when selecting staff for a SOC.

A match between the right people with specific capabilities is crucial for an adequately organised SOC. The same holds for the selection of the very people who are able to cope with change (see Chapter on People).

In a traditional r-SOC the IT-manager is the most important stakeholder. He is responsible for a reliable infrastructure. Next to him the compliance officer plays an important role within a traditional r-SOC.

In a modern p-SOC, when the total threat assessment of a business is analysed, among other things based on a current, operational threat assessment, even the business becomes a stakeholder of SOC. The business wants to have insight into the quality of IT services rendered and their safety (they are looking for a dashboard). Risk Reduction is an important business driver for them.



**Figure 5:** Represents schematically the factors that influence a modern p-SOC (Rob van Os based on 'Figure 1' p. 14 - *Ten Strategies of a World-Class Cybersecurity Operations Center*).

An important question that should be answered in a modern p-SOC is who in the business is in charge as regards education if IT and security are involved? What knowledge should they have? This is important for both the business and the SOC if they want to perform to the best of their ability. True enough, in case of an incident SOC cannot deal with everything, the business itself should take action as well.

In order to make sure communication between the business and SOC runs smoothly, a choice can be made to appoint ambassadors who get a role to work on behalf of SOC in the business and vice versa. In this way, mutual understanding and support for change will be created.

### 3.3 The human factor within a SOC

It has been mentioned before that our view is that the human factor determines the success of a modern SOC. Eventually it is the maturity of the staff that is decisive whether it is possible to hit the ceiling using current processes and available techniques.

A very important lesson when selecting the right people for a SOC is that quality, not quantity, is relevant. Using the right tools, one single analyst can do the work of a hundred or so analysts of average quality. In the book *Ten Strategies of a World-Class Cyber Security Operations Center* it has been described as follows:

*'Analysts can be trained to use a tool in a rudimentary manner, they cannot be trained in the mind-set or critical thinking skills needed to master the tool.'*

A good analyst understands the output of a tool: he/she knows the formation of the output and the context at the time of formation.

### **“Analyst quality is vastly more important than analyst quantity”**

In *Ten Strategies of a World-Class Cyber Security Operations Center* the search for the right people for a SOC has been described as follows:

*‘Perhaps the number one quality to look for in any potential hires to the SOC is their passion for the job, regardless of the position. Intrusion monitoring and response is not just ‘a job’ where people put in their eight- or 12-hour shift, collect a pay check, and then leave. When it comes to ‘cyber,’ we’re looking for enthusiasm, curiosity, and a thirst for knowledge. This passion is what will keep them coming back to the job, day after day, despite the stress and challenges inherent in operations. This passion, along with intellect and other soft skills, is what propels fresh recruits into becoming what we will call ‘rock-star analysts.’*

When you are in the happy position to have collected the right people, the next step is to secure these people for your organisation, a process that Human Resource management plays an important role in. However, it is equally important to watch very closely that these people are challenged all the time, because for some capabilities SOC-work may become routine.

When offering sufficient challenges to the diamonds in your team, you should think of ever recurring activities within the context of monitoring & response, attack simulation & hunting threats. You could even think of a national or international competition of SOCs.

It is certainly possible to tie the right people to your organisation for a longer period in this way, especially when you combine this with a customized development plan. However, it should not be forgotten that after five years or so many people will leave, because they feel that by then they have seen it all. Common sense, though, will restore proper dynamics within a SOC. Indeed, new people with new educational skills, such as data analysts, will render new insights.

Within organisations there is not yet enough focus on advancement and development of SOC-employees elsewhere in the organisation. They might be in a favourable position to take on the role of ambassadors. This is an important point of interest that HR might or should play a role in. There is much talk of Job Rotation, but as yet it is hardly applied.

Nb. In general it may be stated that it is not easy to select the rightly trained candidates, seeing the rapid developments that SOCs are confronted with now. This does not apply to the necessary ‘blue’ people, who are responsible for structure within a SOC-team, but it surely holds true for the ‘yellow’ extrovert creative people, who bring the necessary balance within a team and who realize future viability. It is often exactly these creative members that show the desired adaptability to operate in the evolving environment of a SOC.

### **3.4 Processes within a SOC**

From a SOC point of view four main processes within a SOC should be shaped:

- Threat Intelligence: to get an insight in what is happening in our environment and in the world around us.
- Vulnerability Management: testing, monitoring and problem-solving vulnerable items in information systems.
- Security Monitoring: a 24/7 monitoring on deviations and attacks.
- Incident Response: the process to deal with disturbances and attacks in the organisation directed by SOC.

The processes that play a role within a SOC are strongly connected with the two mutual goals that many SOCs have:

1. Get an insight in Situational Awareness.
2. Focus on Incident & Response in the interest of the business.

The basic shape of the threat intelligence process within the context of obtaining SA is as follows:

1. **Collecting data**  
Joining information from various internal and external sources and enrich them, if necessary, with internal information, such as a configuration data base and threat intelligence sources.
2. **Triage and converting in actionable items**  
Assessing and analysing of raw data on relevance for the home situation in a structured way, such as a more thorough analysis of the retrieved data or collecting additional data.  
Specific information can be turned into action on the spot, such as patching systems, adapting detection regulations in SIEMs, checking IOCs (Indicators of Compromise) and so on.
3. **Communication and sharing**  
Depending on positioning of SOC and the extent of involvement with other communities, among other things, it may be desirable, or even necessary, to (partly) share analyses with third parties. It is of importance to determine which information should be shared and for what reason. Dependent on the nature of the communication it may even be necessary to deliver a contribution by functioning as a source of Threat Intelligence for third parties.
4. **Creating a threat assessment and report**  
In this process, it is important to create a (real time) assessment on defensibility of the organisation based on diverse information obtained by Threat Intelligence. This threat can also supply the business with the necessary alertness when executing business processes.

In the context of Incident & Response the current processes can be easily represented in a scheme. In this case, it is a matter of the ongoing Prevent-Detect-Response cycle that always follows the process of Identifying:

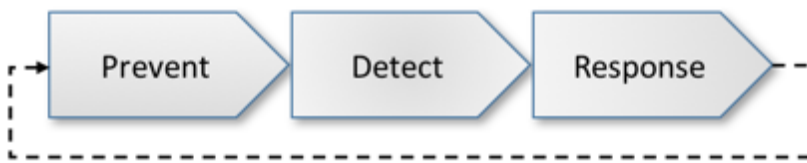


Figure 6: The ongoing Prevent-Detect-Response cycle (Source: page 3 The Next SecOps Fundamentals)

In this cycle response may be split up into processes of: repression (damage control) and recovery (damage repair).

The reporting process is very important in this cycle. Who is in charge to control whether automated decisions and/or actions are correct? This is a key point of attention to evaluate effectiveness and reliability of a SOC.

In order to obtain insight into Situational Awareness as well as to enlarge the Incident and Response capability, it holds true that processes to realize these goals can be set up in two ways: 'Mode 1' that symbolizes the 'solid as rock' old legacy systems and 'Mode 2' that represents a much more dynamic, agile approach. In defining 'Mode 1' and 'Mode 2' Gartner's definitions of these notions are being used.

- In 'Mode 1' work is carried out in a rather stable environment, using quite old systems with hardly changing functionality. Security monitoring may be simple, because it can quickly be determined what is regular and what is not in the systems used. Besides, vulnerability management is easy: all systems are well-known. These systems are partly outdated, however, not much is changing. The moment it is clear what systems are being used, inclusive of their operating systems, versions and patch levels, a new CVE can easily be mapped on relevance. However, it is true that we run the risk that security patches for old systems will not be available anymore. If this is the case, vulnerability management has become hardly possible anymore and what remains is to patch virtually or to implement complementary security measures, if possible.
- In a 'mode 2' environment that is much more dynamic in users, systems and functionality, it is necessary to put more energy into adequately embedding security monitoring and vulnerability management. What is needed is a capacity to quickly switch to change and to monitor new vulnerabilities. In a 'mode 2' environment mapping new CVE has become more complicated, just as monitoring security. In this environment, it will be more difficult to determine abnormal behaviour and deviations. After all, it is hardly possible to follow normal behaviour. In order to be capable to switch to changes swiftly and flexibly, an organisation should develop more and more into a 'mode 2' environment. Not only does this require a different

approach of the main processes in a SOC, but also of the four other pillars: capabilities, organisational structure, people and technology.

### 3.5 Use cases

In this article, we want to pay attention to the process of developing use cases for a SOC. This is an activity that should start from a threat. An answer should be found to questions such as: What are we afraid of? What threats constitute risks for us and for the business? What risks do we want to mitigate? What do we want to know? How will we determine what we want to know? What information do we need? Is this information available by means of the current applications? What signals are important enough to respond to? Who does what and when?

In order to obtain information from an existing environment, it may be necessary to place security sensors in the network such as Firewalls, Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS) / Data Loss Prevention (DLP) software or agents on servers. In some cases, applications must be adapted so that the necessary log information can really be produced by the application.

This process, as described above, has been represented in Figure 7:

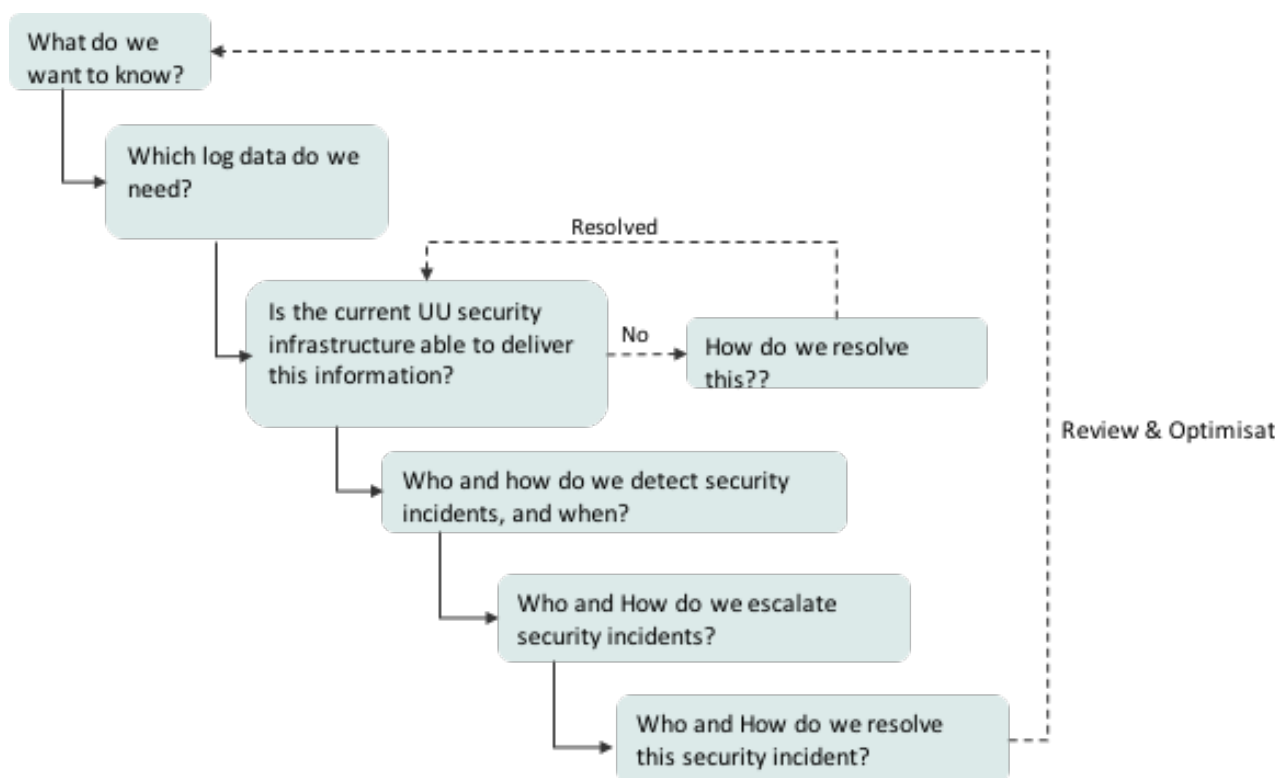


Figure 7: Use case development process (Renato Kuiper, courtesy of Wilco van Ginkel).

Setting up a use case simultaneously answers the question who is going to do what and when. This is certainly helpful if a MSSP (Managed Security Service Provider) will be chosen to deliver services on behalf of SOC. In this case SOC-governance on a tactical and operational level has already been described for these use cases.

Every use case starts from a possible scenario that may occur. This scenario is described and mapped on infrastructure and/or application on the spot where it may occur.

Activity	People	Technology	Process
What do we want to know?	<b>Digital examination</b>		
What log data do we need for that?	Organization and Remindo	Data log and Syslog	Organization-log analyse process
Can the current UU security infrastructure deliver that data?	IAM system log/ Remindo Database log	Not yet, but it is possible → investigate.	
Who and how do we detect security incidents and within what timeframe?	Teacher, observer: real time observations in room.		Remindo and MSSP
Who and how do we escalate these security incidents?	Available staff and Remindo? Functional maintenance group.	Organization-CERT: mail or telephone	Escalation process of MSSP.
Who and how do we solve this security incident?	Remindo and Organizational technical support	Depends.	Organization-Incident process
Review and optimization: what do we need to make it better to detect it earlier?	Possible adjustments: Active monitoring	Possible adjustments: Tooling	Possible adjustments: Yes

Figure 8: Use case description (Renato Kuiper, courtesy to Wilco van Ginkel).

Various scenarios now can be described, as represented in figure 9.

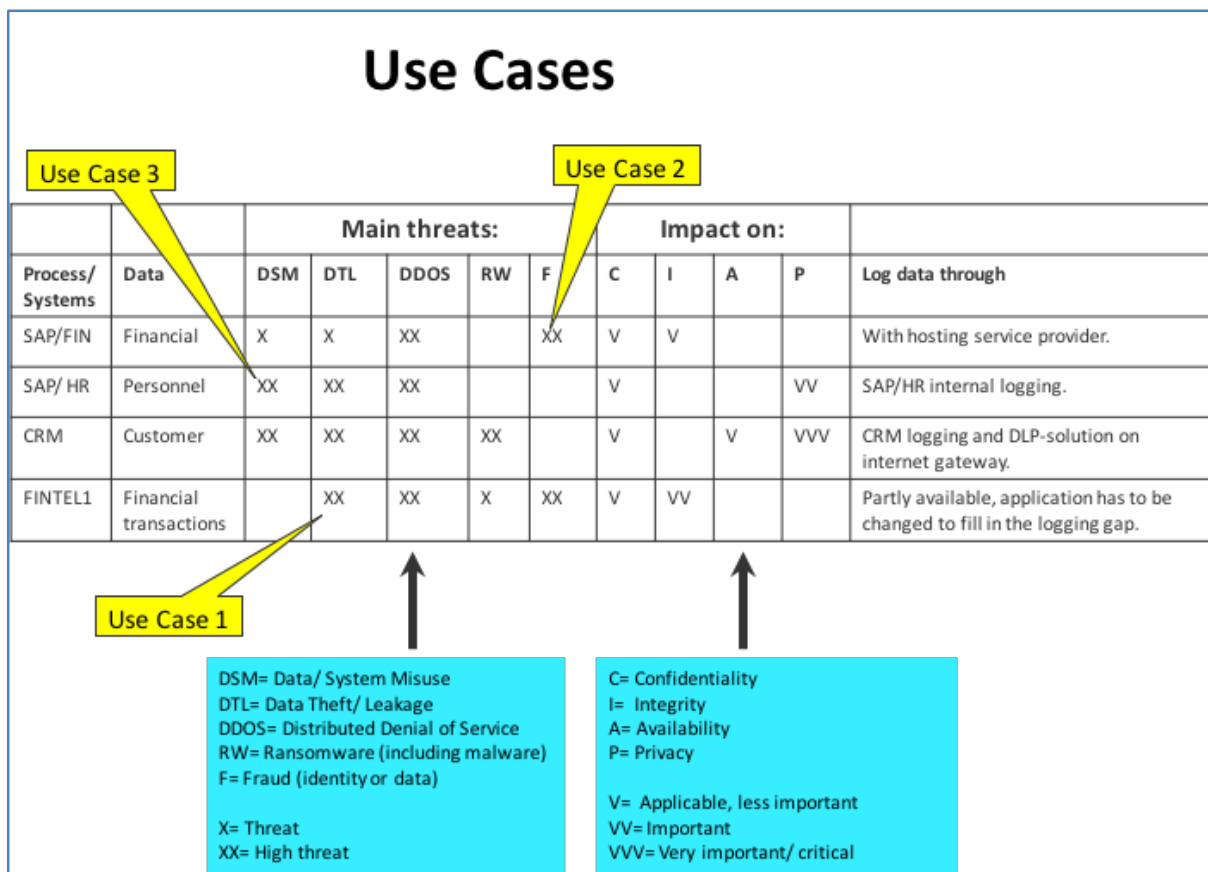


Figure 9: Use case (Renato Kuiper, taken from a real-world case in The Netherlands, courtesy of Wilco van Ginkel).

Every use case must be evaluated on being correct and efficient. Changes in threats may lead to adaptation of an existing threat assessment or to removing an existing use case, even to setting up a new use case.

What holds good for all use cases is that it is a matter of just beginning at these use cases that might work. Therefore, opt for these use cases that show a clear threat and that have owners of this threat (preferably business owners). Opt for threats that can be solved in an unambiguous manner, but most importantly, use threats that are well-documented. Start with a limited number of use cases and gather experience. In figure 9 this has been represented by selecting only three use cases from a list of fifteen use cases.

### 3.6 Technological approaches within a SOC

Even in a p-SOC technology from an r-SOC is still present, such as a SIEM, or log-in information from security devices, such as firewalls, IDS, DLP and so on. Seeing the ever-expanding amount of data (Big Data) and threats that SOC's are confronted with, a further automation of workload is necessary. Think of technics such as 'Machine Learning' (ML), 'Artificial Intelligence' (AI) and 'Deep Learning' (DL). It is no solution to take on more staff. After all, the amount of data will keep growing and it is impossible to expand a team again and again. Moreover, this is not what should be aimed for, because unchallenging work that can be automated should not be done by people. It should be kept in mind, however, that it is important who controls the correctness of automated decisions



and actions and whether they comply to the rules. Big Data requires specific new specialists and technology in the field of data science, as a supplement to a flexible, modern SOC-team.

Another development that can be observed is the rise of 'Threat & Security Intelligence'-technology, such as 'threat hunting' and 'red teaming', in line with a development from reactive to proactive. These techniques do not replace monitoring, but complement it. The aim of 'threat hunting' is to detect threats that are hitherto unknown. 'Red teaming' not only demonstrates vulnerabilities in the infrastructure or the human factor in the organisation, but reaches further by assessing dynamics between attack and defence, in this case the incident response team. Hence, 'Red teaming' is a complete simulation of a cyber-attack. A shift from traditional pen-testing to 'Red teaming' can be seen. It is advised, however, not to undertake 'red teaming' on your own, but to involve a third party in order to prevent tunnel vision.

Of course, a SOC itself can test all kinds of scenarios in a so-called try-out environment, which certainly is a way to keep employees motivated. If few incidents arise, controlled incidents can be created to keep people focussed. Simulation techniques and simulation experts, for instance, should certainly be asked to cooperate.

## 4. MATURITY OF A SOC

Agility of a SOC while maintaining customer services requires a certain degree of maturity, involving for a SOC to function in a controlled way and to be directed. Continued growth and moving along with the latest developments in cyber security, both in terms of threats and in technological developments, are components of maturity.

Measurements should be carried out regularly in order to determine the degree of maturity of a SOC. These measurements enable the organisation to identify weak spots, to determine concrete subsequent steps and eventually to demonstrate the growth in maturity.

To carry out these measurements a model has been developed that sees to crucial elements in the domains that were dealt with in the previous chapter. This model is called SOC-CMM and is loosely based on the traditional capability maturity model. The main difference is that this model is specifically targeted for SOC's and supports organic growth instead of growth in defined plateaus. Figure 10 shows the aspects that can be measured in this model.

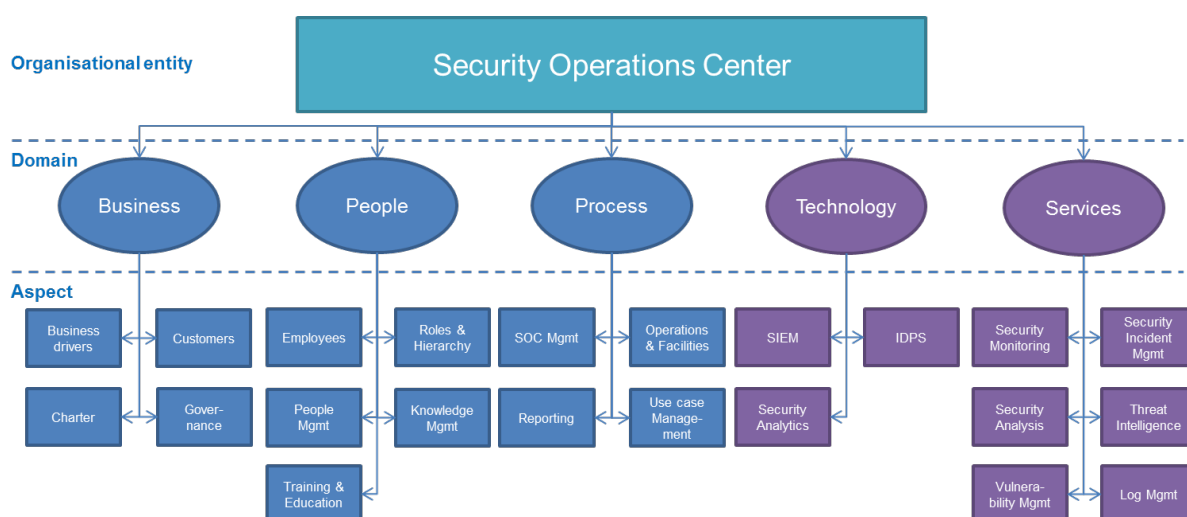


Figure 10: SOC maturity elements (Rob van Os).

Domains that maturity is measured in have been indicated in dark blue, domains that measure both maturity and technical aspects have been indicated in violet.

To determine the level of maturity and capacity within a SOC-CMM, a self-assessment can be carried out. A template for this assessment is to be had for free on the SOC-CMM site (<https://www.soc-cmm.com/>). Using this self-assessment, preferably in the form of a workshop, a SOC can be inspected in width and depth. It is easy to carry out a self-assessment and it is cheap as well, moreover, it gives a good impression of a SOC relatively quick, provided the suitable persons have joined the workshop. The disadvantage of such a self-assessment is that a certain form of subjectivity may occur. Therefore, it is wise to use an independent facilitator who has a keen eye for objectivity and sees to it that everyone can contribute adequate input during a workshop. Such a facilitator can be someone from within the department who is not involved in the actual discussion, or someone from outside the department, or even someone from outside the organisation.

When completing the first self-assessment of maturity in a SOC (baseline) the starting point of a SOC will be determined. From this starting point onwards, a growth path can be laid out that matches the level of ambition of the SOC and the context of the organisation. It is essential to realise the intended growth in a controlled manner. There should be a good balance between the processes concerning the current operation on the one hand, and realisation of innovation and growth to maturity on the other hand. Hence, choices should be made as regards focus. First of all, it is customary that investments will be made on elements that a SOC feels as most important and on elements that lag in maturity or elements that might be missing altogether. By repeating these assessments regularly, it can be determined whether the objectives set have been realised and the correct path has been followed. Therefore, it is important to specify these objectives after the baseline measurement.

Finally, it is important to organise growth in maturity in such a way that agility remains central. There is a risk that agility will get lost by a rigid attitude towards maturity, especially if it concerns regulatory burdens of a SOC. In the long term this may block further growth and development.

## 5. TRENDS & DEVELOPMENTS

The most important trends in the context of the development from an r-SOC to a p-SOC have already been stated:

- From reactive to proactive.
- From detecting only familiar threats (r-SOC) to simultaneously searching for unknown threats (p-SOC). Think of the rise of threat-hunting, for instance.
- New methods such as ML (Machine Learning), AI (Artificial Intelligence) and DL (Deep Learning) are being introduced, now that more types of information are gathered within SOC's. This is a development that really fits the objective of a SOC to create increasing value for the business.

In addition, a development can be seen that a SOC is currently being structured more and more bottom-up instead of top-down, interwoven with a development from reactive to proactive. This means that a SOC itself places spearheads on the agenda, thus requiring selecting more people within the team who are creative and fine-tuned to business. These creative people flourish in a bottom-up structure, also named a team-based structure. The role of the SOC manager in such a structure is to monitor the balance in the team in order to get the best out of it.

Another important trend that experts have observed is the necessity to cooperate. It is very likely that a certain threat has also been detected somewhere else, so it is important to exchange information. For this reason, public-private partnerships such as ISACs (Information Sharing and Analysis Centres) are very important. These are partnerships that exchange information and experiences as regards cyber security and share analyses, predominantly on a tactical level.

In the Netherlands, we have the following ISACs:



Figure 11: Existing ISACs (source: <https://www.ncsc.nl/samenwerking/isacs.html>)

Concluding, some noticeable developments from the *Cyber Security Assessment Netherlands 2016* report (<http://www.ncsc.nl>) to be mentioned: (The report was presented by the NCSC in September 2016)

- Professional criminals carry out prolonged, high quality and sophisticated operations.
- The competitive position of The Netherlands is under pressure due to digital economic espionage by foreign intelligence services.
- Ransomware has become common and more advanced.
- Advertising networks have not yet been capable of coping with malvertising.

Secretary of State Klaas Dijkhoff of the Ministry of Justice classified these developments as critical at the presentation of the NCSC report. He sees these developments as a reason to pay extra attention to ‘digital dike monitoring’, the National Detection Network (NDN) that has been set up to further communication on imminent threats between government and companies.

Source: [www.ncsc.nl](http://www.ncsc.nl)

## 6. REFLECTION

Concluding, within a modern p-SOC human beings are leading, as opposed to a traditional r-SOC that was technology-centred. A modern p-SOC no longer is an accumulation of technical solutions and certainly is not to be compared to a SIEM as of 2017.

The human factor is all-decisive for the success of a modern p-SOC. A success that in the end is determined by the potential to be able to adapt to a fast-changing society in the outside world. Human beings should indicate priorities as well as decide whether an alarm must be responded to, based on the context of this alarm.

Of course, dull and repetitive work should be automated, if possible. However, systems learn from rock star analysts in the end. Moreover, these analysts control if automated activities work out correctly.

Finding these rock star analysts remains difficult. Therefore, experts keep on hammering home the need for internal training, even more so given the fast-changing playing field of a SOC. However, bulky educational organisations often have difficulty to adapt to these rapid changes, so on-the-job training is crucial, even more so to keep staff motivated.

## 7. THE WAY FORWARD

Developments to support automated defence, such as Machine Learning, Artificial Intelligence, IoT, Data Science and, for example, Auto morphing will go on. An agile modern p-SOC should be prepared for these developments. The same holds for the ongoing professionalization of adversaries. It is obvious that a p-SOC is no final stage. Agility in combination with human action remain essential, even if a further development to a tactical SOC, a t-SOC, will be the next step in the foreseeable future.

### Characteristics of a t-SOC:

- A t-SOC will move on to a proactive and predictive focus, complemented with radically automated response.
- A t-SOC goes beyond traditional infrastructure logging and uses Big Data solutions to be able to apply effective monitoring in a diverse application landscape.
- A t-SOC can carry out threat hunting in an extremely dynamic environment: initially fed by mode 2 IT and probably later fed by automated defence.
- A t-SOC is supported by a hybrid team of employees. This team unites infrastructural expertise as well as applicable security, Big Data expertise and business interests.
- Tasks that are operational and repetitive will be automated more and more. It may be questioned whether a t-SOC still is an 'operational' entity? It seems more likely that a t-SOC will rise above this role and will fulfil a more tactical role within the organisation. Threat management and SA, both supported by threat intelligence, will be prominent in this process of transition.

### Conclusion / Takeaways

- Whether a modern p-SOC is successful or not will be determined by the right people. A modern and agile SOC will be predominantly centred on people's effort, as in the end it is and will be a human decision to act upon an alarm. Only a human being can assess the broader context of an alarm, though technically supported. Eventually human specialists will check if automated activities turn out as they are intended.
- A modern p-SOC is dynamic by its very nature. The degree of agility in an ever-changing field does essentially bring out the power of such a SOC. It is this factor of agility that is conclusive in selecting the right people in a SOC. Take care to combine 'blue' and 'yellow' employees who unite infrastructural expertise as well as applicable security, Big Data expertise and business interests.

- In some cases, SOC-work can become boring and therefore it is essential to pay attention to offering challenges in order to keep employees captivated. Sound people management is required to achieve this. Consider that a certain degree of employee turnover is beneficial for an organisation. After all, new employees offer new, fresh insights. Bear in mind that ex-colleagues may become ambassadors in the business for SOC and vice versa.
- When objectives and ambitions are being determined, it is important to realize that it is not possible to carry out every task within a SOC. Therefore, having a focus when determining Incident and Response capabilities is essential. Take care to fine-tune with the business all the time. There is no 'one size fits all'. Therefore, make up your mind and appoint ambassadors who work vice versa and so can fulfil a role within a SOC as well as in the business and in this way, can create mutual understanding and support.



## APPENDIX 1: BIBLIOGRAPHY

The expert group recommends the following literature, in addition to the topics covered and for further intensification:

Title	#pages	Relevant pages	File name	Author
Ten Strategies of a World-Class Cybersecurity Operations Center	346	vii (table of contents)	01-pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf	MITRE
Ten Strategies of a World-Class Cybersecurity Operations Center	346	81-85		
Cyber Resiliency Engineering Framework	78	Chapters 3 and 4	02-MITRE-Cyber resilience engineering framework.pdf	MITRE
Cyber security information exchange to gain insight into the effects of cyber threats and incidents	9	Full article (especially the section on impact)	03-Artikel - Springer Cyber information exchange to gain insights.pdf	Fransen, Kerkdijk, Smulders
SOC Expertbrief	10	All	Expert Brief - SOC V1.0 definitief.pdf	Previous group
SOC notes Ben, kelvin, Renato Andre			Work document SOC XP brief 20140901.doc	Ben, Andre, Kelvin and Renato
On SecOps Maturity	8	Full paper	Seculior - On-SecOps-Maturity-June-2016.pdf	Wilco van Ginkel
The Next SecOps Fundamentals	8	Full paper	Seculior - The-Next-SecOps-Fundamentals.pdf	Wilco van Ginkel
Security operations services (Rabobank)	2	Both sheets	Security Operations Services - obo XP brief SOC.ppt	Kelvin Rorive
SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers				Rob van Os

## APPENDIX 2. INFORMATION ON PARTICIPANTS

Participants who have contributed to this expert brief have been listed below. Contact with (one of) them can be realised through the PvIB Secretariat (see <http://www.pvib.nl/contact>).

### Renato Kuiper



Security architect at Verdonck, Klooster and Associates. Works at the intersection of information security, risk management and architecture. Starting from these perspectives he has gathered experience in Security Operations Centres.

### Sandra Kagie



Self-employed copywriter/journalist. In the past she was closely involved as copy editor for 'Informatiebeveiliging', the Dutch language magazine of PvIB. <http://www.sanscriptproducties.nl> / Twitter @SanSanscript.

### Kelvin Rorive



Together with an international team responsible as manager within Rabobank's Cyber Defence Centre for global IT threat management, security monitoring and Incident Response. He also serves as chairman of PvIB's event committee.

### Charlotte Rutgers

Senior innovation manager at the Ministry of Defence. Worked in the past as acting security officer in a SOC.

### Andre Smulders



Strategic Advisor Cyber Security. Works at TNO on security innovation for ordering parties both private and public. Is co-author of 'Foundations of Information Security - based on ISO/IEC 27001 and ISO/IEC 27002'.

### Ben van Zuijlen



Manager of Volksbank Control & Security Center and ultimately responsible for Security Operations Center activities. Also vice chairman of FI-ISAC.

### Rob van Os



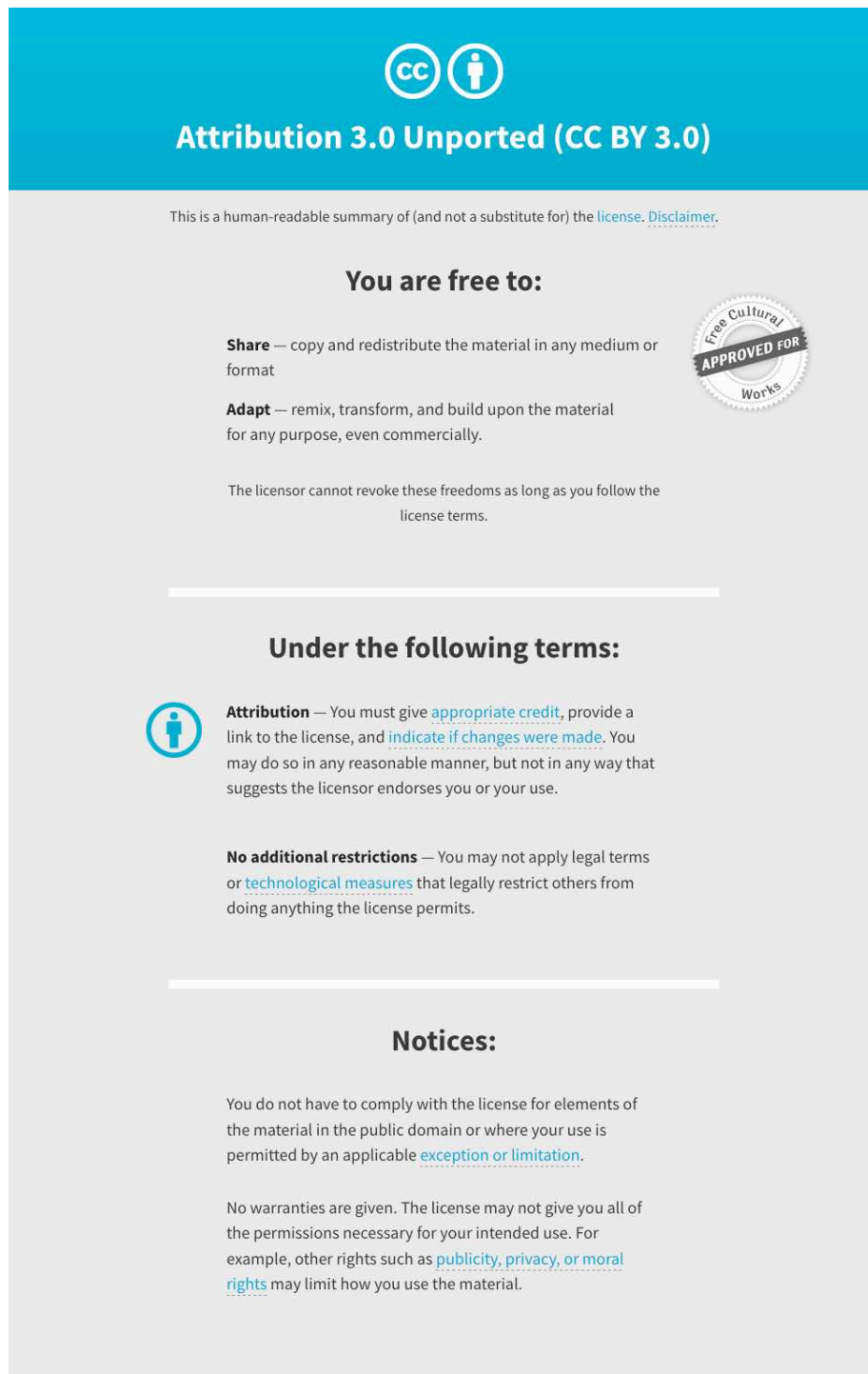
Cyber defence specialist at Volksbank. Responsible for operations as well as growth and maturity for the Security Operations Center. As a consultant he gained experience in SOC processes and organisation of a SOC. He is also the author of the SOC-CMM.

## APPENDIX - APPLICABLE PUBLICATION LICENSE

The Expert Brief is published under the following license:

<http://creativecommons.org/licenses/by/3.0/>

At the time of writing this page showed:



The image shows a screenshot of the Creative Commons Attribution 3.0 Unported (CC BY 3.0) license summary page. The page has a blue header with the CC logo and a person icon, followed by the text "Attribution 3.0 Unported (CC BY 3.0)". Below the header, there is a disclaimer: "This is a human-readable summary of (and not a substitute for) the license. [Disclaimer.](#)". The main content is divided into three sections: "You are free to:", "Under the following terms:", and "Notices:". The "You are free to:" section lists "Share" and "Adapt" permissions. The "Under the following terms:" section lists "Attribution" and "No additional restrictions". The "Notices:" section contains two paragraphs of text. A circular seal on the right side of the page reads "Free Cultural Works APPROVED FOR Works".

**CC BY**

### Attribution 3.0 Unported (CC BY 3.0)


This is a human-readable summary of (and not a substitute for) the [license](#). [Disclaimer.](#)

#### You are free to:

**Share** — copy and redistribute the material in any medium or format

**Adapt** — remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms.



#### Under the following terms:

**Attribution** — You must give [appropriate credit](#), provide a link to the license, and [indicate if changes were made](#). You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

**No additional restrictions** — You may not apply legal terms or [technological measures](#) that legally restrict others from doing anything the license permits.

#### Notices:

You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable [exception or limitation](#).

No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as [publicity, privacy, or moral rights](#) may limit how you use the material.

## **BECOME A MEMBER OF PvIB, PLAY IT SAFE AND SECURE TOGETHER ...**



**Information security has been a necessary, exciting and dynamic specialism for years now. Almost all professions now, more than ever before, are confronted with confidentiality, availability and integrity regarding information, no matter whether they work as CEOs, managers, consultants or programmers. The Platform for Information Security offers to be of help and to support you in all problems in the field of Information Security.**

### **What is the Platform for Information Security?**

The PvIB is a freely-accessible, broad platform for professionals who meet each other to professionally approach Information Security by exchanging ideas, information, know-how, insights and by sharing practical experience.

### **What does the Platform for Information Security aim to achieve?**

The Platform aims to advance the physical, (system) technical and organisational security of data and data-processing instruments and aims to offer protection against threats from within or from outside. We also want to advance the exchange of knowledge and experience by professionals working in the field and inspire them to set up networks, possibly by means of this Expert Brief.

### **Target Group**

The target group of PvIB includes every person who is involved in Information Security, either by profession or by study as well as every person who takes a special interest in Information Technology. Our fast-growing membership contains many disciplines such as students, information architects, technicians, managers, consultants, lawyers, security officials and IT auditors. Our members stem from a variety of educational backgrounds, companies, (regional) government, organisations and suppliers.

For the various possibilities to become a member of PvIB, you are kindly referred to:

<https://www.pvib.nl/abonnementsinformatie>