2015 48th Hawaii International Conference on System Sciences

A framework for Designing a Security Operations Centre (SOC)

Stef Schinagl BBA QSA CISA
Noordbeek
stef@noordbeek.com

Keith Schoon BSc QSA CISA
Noordbeek
keith@noordbeek.com

prof. Ronald Paans Ph.D
Noordbeek and VU University Amsterdam
Ronald.Paans@noordbeek.com

Abstract

Owning a SOC is an important status symbol for many organizations. Although the concept of a 'SOC' can be considered a hype, only a few of them are actually effective in counteracting cybercrime and IT abuse. A literature review reveals that there is no standard framework available and no clear scope or vision on SOCs. In most of the papers, specific implementations are described, although often with a commercial purpose. Our research was focused on identifying and defining the generic building blocks for a SOC, to draft a design framework. In addition, a measurement method has been developed to assess the effectiveness of the protection provided by a SOC.

1. Introduction

Society is continuously under attack from hackers, criminals and other malicious actors. For example, an attack on the Dutch SSL certificate provider Diginotar succeeded in June 2011. The attackers collected the private keys and issued rogue certificates that were later abused in a large scale attack in August of 2011 [3]. This attack damaged many government agencies, forcing them into expensive replacement of all SSL certificates.

Citizens and organizations are rapidly becoming more vulnerable to cyber-attacks because of increasing dependency on vulnerable techniques. An example is the chip for e-ticketing for national public transportation, the OV-chipkaart, which was successfully hacked several times between 2007 and 2011, allowing travelers to manipulate their accounts and to travel for free [11] [4]. Other examples are the online Dutch payment system IDEAL for bank transactions and the citizens' identity verification DigiD; both attacked via DDoS. The increasing number of attacks is also observed by the Dutch National Cyber Security Centre [10] [15] [7]. Society's increasing dependence on IT results in more severe consequences when IT fails to function.

This awkward situation was made worse by the financial crisis as budgets were cut and unemployment rose, having adverse effects on cybercrimes in many ways. Firstly, private and public organizations spend less modernizing IT and improving information security. Secondly, a crisis makes it easier for criminal groups to recruit skilled employees since the group of unemployed and perhaps vengeful and unhappy people is growing [7]. In addition, citizens feel uncertainty that is abused by cybercriminals via finance related attacks [1].

In response, many organizations are trying to protect their business processes by implementing additional measures for information security. One of these measures is setting up a Security Operations Centre (SOC), assuming this would be the solution to counteract cyber-attacks and abuse. These organizations are faced with a real challenge: the absence of an explicit model and guidance on how to establish a SOC. Each organization has to re-invent the wheel, leading to a diversity of implementation forms, and high costs.

A number of papers from leading security suppliers [13] [5] [6] [8], describe specific implementations and are written with a commercial intention. An organization that has to build its own SOC has little benefit from these papers, since they contain no general guidance.

1.1. Research: A framework for a SOC

Noordbeek collaborated with VU University Amsterdam to investigate common practices for private and public SOCs and to develop a framework for the design and implementation of an effective SOC. This research focused on modelling the structure of a SOC with the goal to assist large companies and governmental agencies in establishing SOCs which can offer effective cyber security to multiple organizations.

For designing our research approach, we used Yin [17]. In this context, we visited a number of SOCs, mapped their activities, measured the effectiveness of their performance, analyzed their problems and developed a generic model based on their common aspects. This model contains five basic elementary functions, called the building blocks of a SOC. This structure was verified in collaboration with the stakeholders from the participating SOCs and was validated by them.

1530-1605/15 $31.00 © 2015 IEEE
DOI 10.1109/HICSS.2015.270

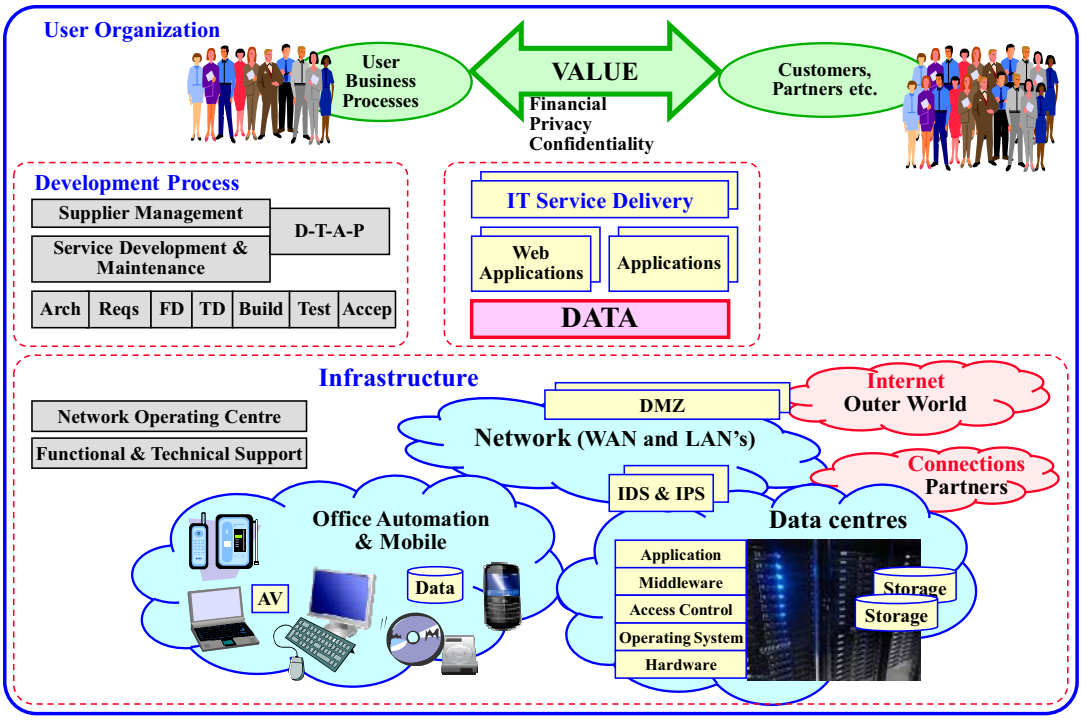

Figure 1. IT Services and their context

The model was presented to the Dutch security community, who recognized and accepted it as a model for designing new SOCs or further improving existing SOCs.

2. Background literature

Businesses are embracing cloud solutions, user mobility, expanding social collaboration, and creating and sharing extraordinary volumes of data [15] [7]. The combination of business and IT transformation, compliance and governance demands, and the onslaught of security threats continues to make the job of safeguarding data assets a serious challenge for organizations of all types [Trust 2013].

2.1. Cyber-attacks

Today's reality is 'no matter what business you are in, no matter where in the world you are if you have got data, your business is at constant risk'. From the outside in, to the inside out threats are increasing as quickly as you can implement measures against them [15]. In a similar way, EY states that 'in today's world of intense use of technology and not enough security awareness on the part of users, cyber-attacks are no longer a matter of if but when'. We live in an age where information security prevention is no longer optional [2]. Attacks are any kind of malicious activity that attempts to collect, disrupt, deny, degrade or destroy information system resources or the information itself. This translates to 137.4 million attacks annually, 2.6 million weekly and 0.37 million daily [6].

The primary data type targeted by attackers in 2012 was cardholder data. Criminals also sought personally identifiable information which has some monetary value, but not as much as cardholder data. Therefore, the primary targets of cyber criminals in 2012 were Retail (45%), Food & Beverage (24%) and Hospitality (9%). Surprisingly Financial Services came fourth (7%) followed by the Non-profit sector (3%) [15].

Cyber-attacks and intrusions are nearly impossible to avoid, given the openness of today's networks and the growing sophistication of advanced threats [14]. In response, the practice of cybersecurity should focus on ensuring that intrusion and compromise do not result in business damage or loss [13]. Preparing for known attacks is hard enough. But, how do organizations build controls for the security risks they do not even know about yet [2]? Some guidance can be found in the publications of the US National Institute for Standards and Technology (NIST).

2.2. Definition of a SOC and its mission

A Security Operations Centre (SOC) functions as a team of skilled people operating with defined processes and supported by integrated security intelligence technologies. The SOC specifically focuses on cyber threat, monitoring, forensic investigation, and incident management and reporting [6], under the umbrella of an overall security operations environment and clear executive support. Without such an umbrella, a SOC is ineffective, and its value is not to be realized. A bottom-up or grassroots approach to security has a minimal chance of survival and an even smaller chance of success [2].

The business interests to be protected by a SOC are depicted in Figure 1. The user organizations and their relations such as customers, partners are essential. They exchange electronic messages and transactions, each representing a particular value. This exchange of information between organizations and there relations can be roughly divided into - more or less - privacy sensitive, confidential, or finance related. The exchange of value between organizations and people is depicted in green at the top of Figure 1. The capability to exchange and process data is provided by IT, with its (web) applications and data storage. From a security perspective, functionality and data are the principal objects to protect. One has to ensure the confidentiality, integrity and availability of IT service delivery.

The applications are acquired via 'make or buy', via Service Development and Maintenance for 'make' and Supplier Management for 'buy'. An increasing number of organizations have adopted methods for Secure Service Development, with sophisticated risk and vulnerability analysis methods, explicit security requirements, involvement of SOC staff for penetration tests and code reviews during the development stages, and security acceptance criteria [9].

A major part of a SOC's attention is focused on the technical infrastructure, with the networks, external connections, office automation, mobile solutions and the servers running the applications and processing the data. The SOC performs continuous monitoring, vulnerability scans, compliance scans, log data collection, etc.

2.3. Detection and Tooling

The primary function of a SOC is continuous monitoring, to become rapidly aware of attacks by malware, DDoS, viruses, hackers, and so on, and paying attention to malicious activities by people such as employees, subcontractors, guests and outsiders. For this, the SOC analysts need to recognize attack patterns, the inherent and specific weaknesses of their own IT infrastructure, the information systems and, the habits and behavior of the regular users.

Organizations must assign highly competent security resources towards rapid threat detection and remediation [13]. A well-functioning SOC can form the heart of effective detection. It can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively [2]. With the understanding that attacks can never be completely prevented, companies should advance their detection capabilities so they can respond appropriately.

Organizations sometimes invest in 'fancy' tooling. The tools are not the Silver Bullet that will protect them from cyber threats outside or already inside the security perimeter [2]. The competences and experience of the staff of the SOC are much more important. Since highly qualified analysts are scarce, this is where organizations struggle the most.

Attacks have grown significantly in complexity, rendering the majority of 'Off the Shelf' detection solutions ineffective [15]. Be aware that some 48% of the tooling belongs to this category. In addition, due to advanced subterfuge techniques, malware often goes unnoticed by system administrators despite being clearly visible to experienced investigators. We have to rely on the human factor, i.e. the analysts, to outsmart the sophisticated attackers.

Security event visualization is still rare in most organizations today. Many security professionals conduct manual log reviews or perform 'spreadsheet' analyses, and for some, implementation of basic Security Information and Event Manager (SIEM) technology is as far as they go. However, the ultimate goal should be to develop an environment in which security events are discovered by security professionals within the organization. Data aggregation or correlation as seen in a SIEM is assumed to be beneficial to real-time security event visualization and notification [15].

2.4. People, awareness and competences

A fundamental component of continuous monitoring is the analysis of data collection, carried out by the analysts working in the SOC [12]. This is a value added activity since highly qualified analysts with acknowledged competences are in charge of both preparation and management of complex security investigations. At the core of a successful SOC is a firm foundation for operational excellence driven by well-designed and executed processes, stable governance, capable individuals and a constant drive for continuous improvement to stay ahead of cyber adversaries [2]. SOCs need collaborative, cross-disciplinary teams with

highly specialized skill sets to combat advanced cyber threats. However, the security community faces a serious shortage of such skills and qualified personnel [13].

Moreover, employees leave the door open to further attacks. Whether it is due to lack of education or policy enforcement, employees happen to pick weak passwords, click on phishing links and share company information on social and public platforms [15].

A complicating factor for establishing cybersecurity is outsourcing. Many third-party vendors do not allow customer organizations to perform logging and monitoring, although their engineers sometimes are leaving the door open for attacks as they do not necessarily keep client security interest in mind [15].

3. Research and measurement method

For the research method, 'Case Study Research, Design and Methods' of Robert K. Yin [17] was used. Yin describes six stages, which we tailored as follows:

Stage 1, the 'Plan' phase has the character of an inventory. We collected literature, visited some SOCs and defined the research question and subquestions.

The central question is: '*What is an effective framework for designing and implementing a SOC to increase the robustness of e-businesses and their customers against cyber-attacks and IT abuse?*' The three subquestions are:

- '*Does literature provide guidance for designing an effective SOC?*'
- '*Which standard functions can be identified when analyzing the design and operations of existing SOCs?*'
- '*How can a SOC provide effective security services to multiple user organizations and IT organizations?*'

Then, we drafted an initial model for a framework, based on input from experts and our expectation of what the common functions should be. This model is used during the interviews and workshops to confirm or reject certain parts of the SOC's functionality.

Stage 2, the 'Design' phase is used to draft a measurement method to assess the effectiveness of a SOC's operations, supported by visual spider diagrams and questionnaires. We made a list of organizations, to visit their SOCs and interview their security staff.

During stage 3, the 'Prepare' phase, we performed a pilot at an organization with a SOC that had already been operating for several years. In close cooperation with the analysts of this SOC and via workshops, we improved the assessment method and the questionnaires, to make them suitable for assessing a multitude of different SOC implementations.

Stage 4, the 'Collect' phase, consists of the site visits, observations, interviews and workshops, resulting in a research database. We discussed the functional building blocks, the existing problems and the current and future objectives with one or more analysts of each SOC and our colleagues.

Stage 5, 'the 'Analyze' phase, is used to finalize the draft theoretical propositions using the quantitative and qualitative evidence collected.

During stage 6, the 'Share' phase, we wrote our report and organized a number of workshops with representatives of the SOCs visited, adapting the draft model until consensus was found. We then presented our research outcome and model to several committees of the security community, who confirmed the model.

4. Observations and analyses

Because each SOC is as unique as the organization it belongs to, it is critical to understand the factors that influence their result. A SOC can include all internal operations, processes, technologies and staff, rely heavily on external provider managed services, or can be a hybrid of out-tasked and internal capabilities. To determine the right balance for an organization, one has to consider cost, skills availability, single point versus multiple global locations, and the importance of around-the-clock coverage and support [6].

4.1. Assessment method

For the assessment method, some of these factores have been combined, and other aspects such as competences, and experience have been added. The questionnaire is divided into four groups, i.e. sharing knowledge, secure service development, continuous monitoring and damage control. The rating per axis is: 1 = unsatisfactory, 2 = concerned, 3 = suboptimal, 4 = satisfactory, 5 = desired level. The rating is relative to the organization's level, i.e. its objective per axis. The visual representation is shown in Figure 2.

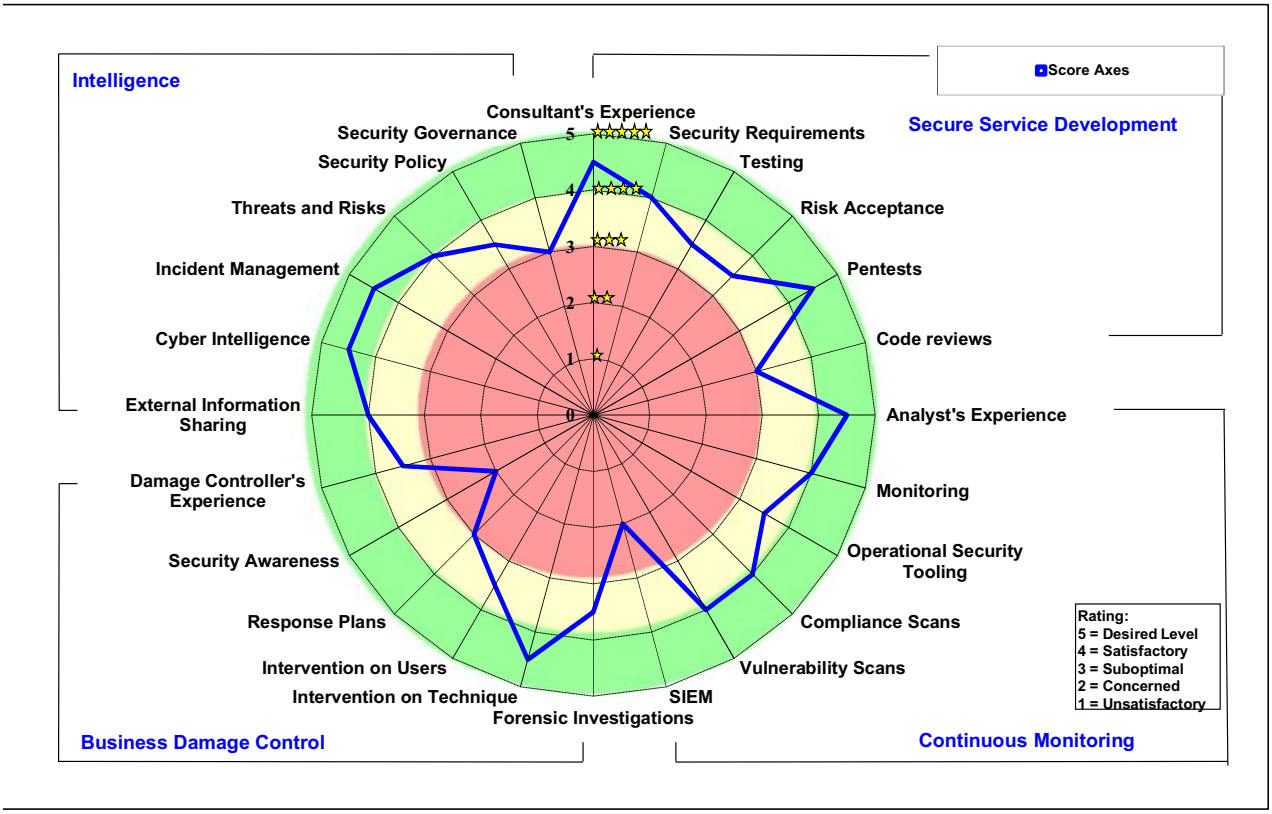

Figure 2. Integral SOC

For each SOC visited, a spider diagram was drafted and discussed with the SOC analysts until it was a reasonable interpretation of the effectiveness of the SOC's operational activities. Using this assessment method periodically, one may monitor the progress of improvement activities.

4.2. Assessment results

Each SOC has a unique design and implementation. Since no generally accepted framework exists, each SOC was formed through organic growth. The security processes are tailored by one or some experts according to the funds and staffing available, on a best effort basis, based on their personal skills and competences. Using opportunities, they created something which is, in their opinion, the right solution for the challenges of their organization.

All of the SOCs were part of or related to the IT department. There are some typical implementation forms, e.g.:

- **Integral SOC**:
  This type of SOC is a center of expertise involved in both secure service development and infrastructure support and operations. We could only find and visit one instance of such an integral SOC during our research. The advantage of an integral approach is that the same analysts and consultants are involved in making new services secure during the acquire phase while later being involved in compliance scanning and continuous monitoring. This is optimal sharing of knowledge;
- **Technology driven SOC**:
  The majority of SOCs is focused on infrastructure support and operations. They are located between functional support, and network and system administrators. This is an effective positioning, since they know what happens in the operational environment and interact directly with the engineers. However, their impact on preventive actions such as making new services secure is limited;
- **Partly outsourced SOC**:
  One SOC consisted of technical security officers, analysts and penetration testers. Because of the infrastructure, scanning and continuous monitoring had been outsourced to the hosting provider. It turns out that knowledge sharing and cooperation had a low rating since human interaction was very limited in this outsourcing relationship;

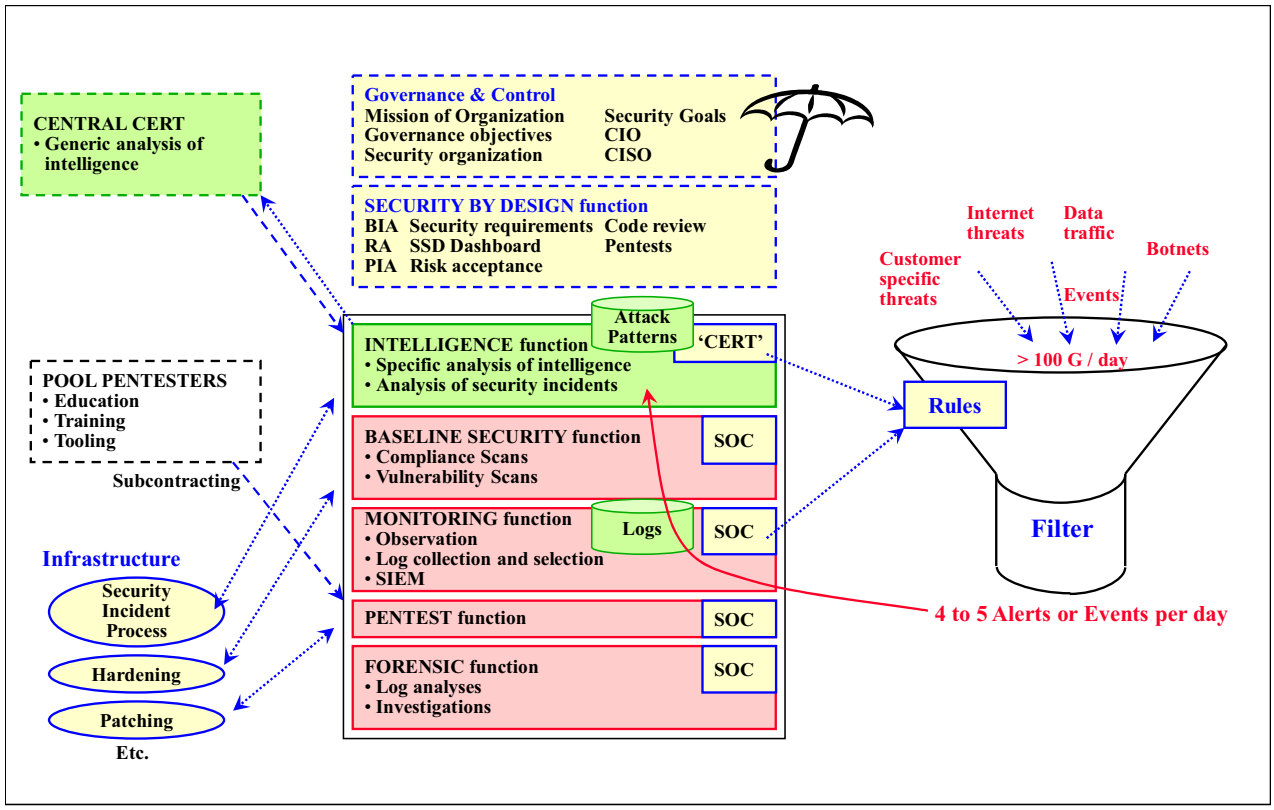

Figure 3. The components of a SOC / Typology

- **Specialized SOC**:
  Some SOCs are highly specialized, due to a particular organization's mission to protect a country and its vital infrastructures. They have experts, e.g., for protecting and guarding Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) computers, and use classified sources for information about threats.

The effectiveness of each SOC is based mainly on executive commitment [2]. Without such commitment, competent resources and sufficient budgets, a SOC can provide 'security in name only'.

5. The framework

A SOC needs an umbrella, consisting of an information security organization with a Chief Information Security officer (CISO), reporting to the Chief Information officer (CIO), and acting within the mission and security goals of the organization.

Moreover, there should be a process for secure service development to ensure that only secure solutions are handed over from the acquire phase to the production environment. In Figure 3, this is depicted as the 'Security by Design' function. This is often combined with methods and processes for Business Impact Analysis (BIA), Risk Analysis (RA) and Privacy Impact Assessment (PIA). These analysis methods provide information about the requirements for confidentiality, integrity and availability.

The research results indicate a clustering of the SOC's activities in five areas, which turn out to be their elementary building blocks. These are:

- **Intelligence function**:
  The kernel of the SOC is the Intelligence function, that shares similarities with a Computer Emergency Response Team (CERT). The competent and skilled analysts are located here, exchanging information with internal and external parties [16], analyzing threat patterns and monitoring results, defining rules for event filtering and giving instructions to operational staff and security staff;

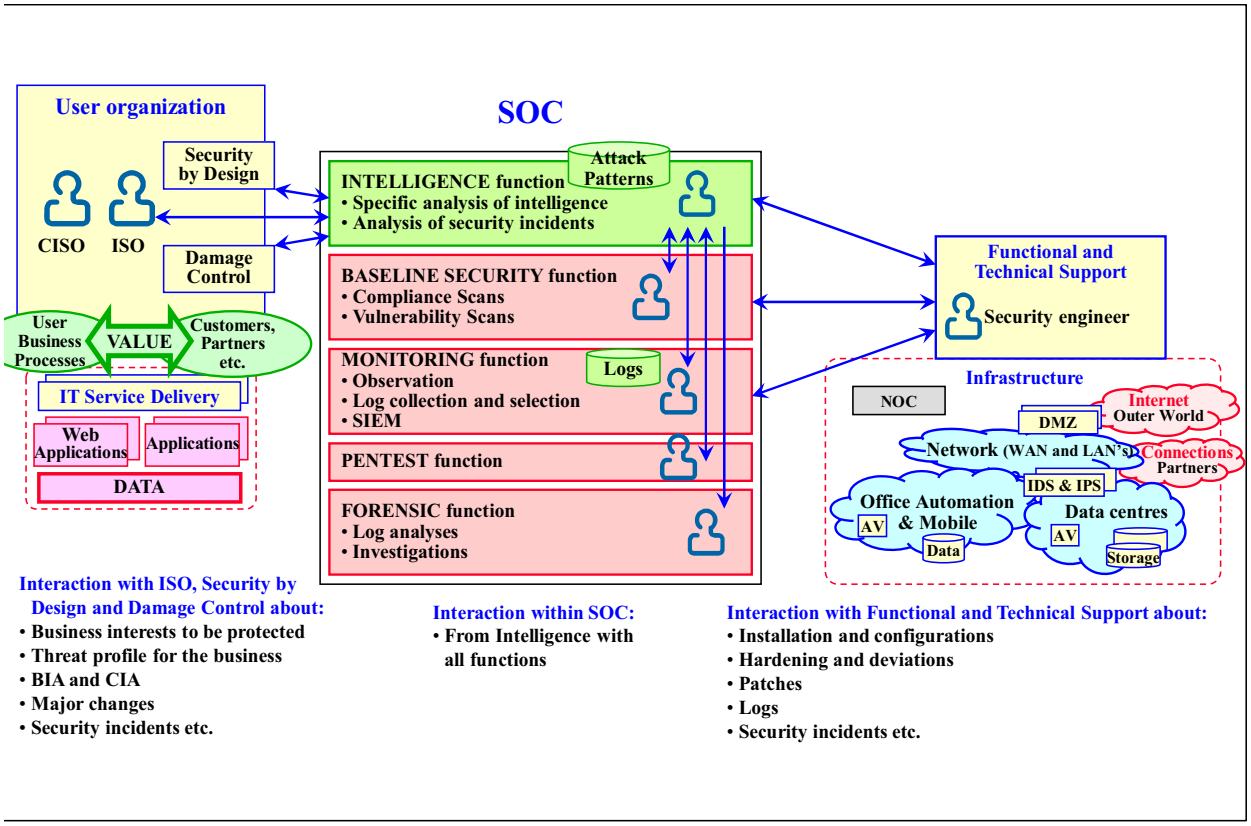

Figure 4. Indivisible relationships: Anchoring a SOC

- **Baseline Security function**:
  The SOC analysts for Baseline Security supervise the operational processes for hardening servers, operating systems and network components, and perform vulnerability and compliance scans to verify adherence to hardening guidelines. Moreover, they scan for known vulnerabilities and verify the maintenance levels based on actual guidance on high priority and security patches. This function also supervises the settings and operational effectiveness of the endpoint protection (e.g. antivirus), firewalls, Intrusion Detection and Protection System (IDS/IPS), Public Key Infrastructure (PKI) etc.;
- **Monitoring function**:
  The SOC Monitoring function observes the data traffic and attempts to identify anomalies. The large volumes of logging data and signals are stored and filtered using dynamic rule sets to find a needle in a haystack. One of their major challenges is to tailor the Security Information and Event Manager (SIEM) in such a way that only the relevant alerts or events are identified;
- **Penetration Test function**:
  Penetration tests are used both as an integral part of secure service development and within the operational environment. A penetration test can determine how a system reacts to an attack, whether or not a system's defenses can be breached, which defenses were defeated and what information can be acquired from the system;
- **Forensic function**:
  The SOCs' analysts are skilled in finding details in the data traffic and logging infrastructure data. When forensic investigations are performed by the Office of Integrity or law enforcement agencies, these analysts assist in collecting electronic evidence and ensuring the chain of custody of such evidence.

For each function, the objectives and activities can be outlined and translated into requirements for competences, experience and number of staff. Here we use rules of thumb, based on observations in existing SOCs.

For instance, experience teaches that seven penetration testers are required for the penetration test function. The calculation is as follows: as soon as a penetration tester has sufficient experience, chances are he or she is offered a job by a specialized security firm with a higher salary than the organization is allowed to

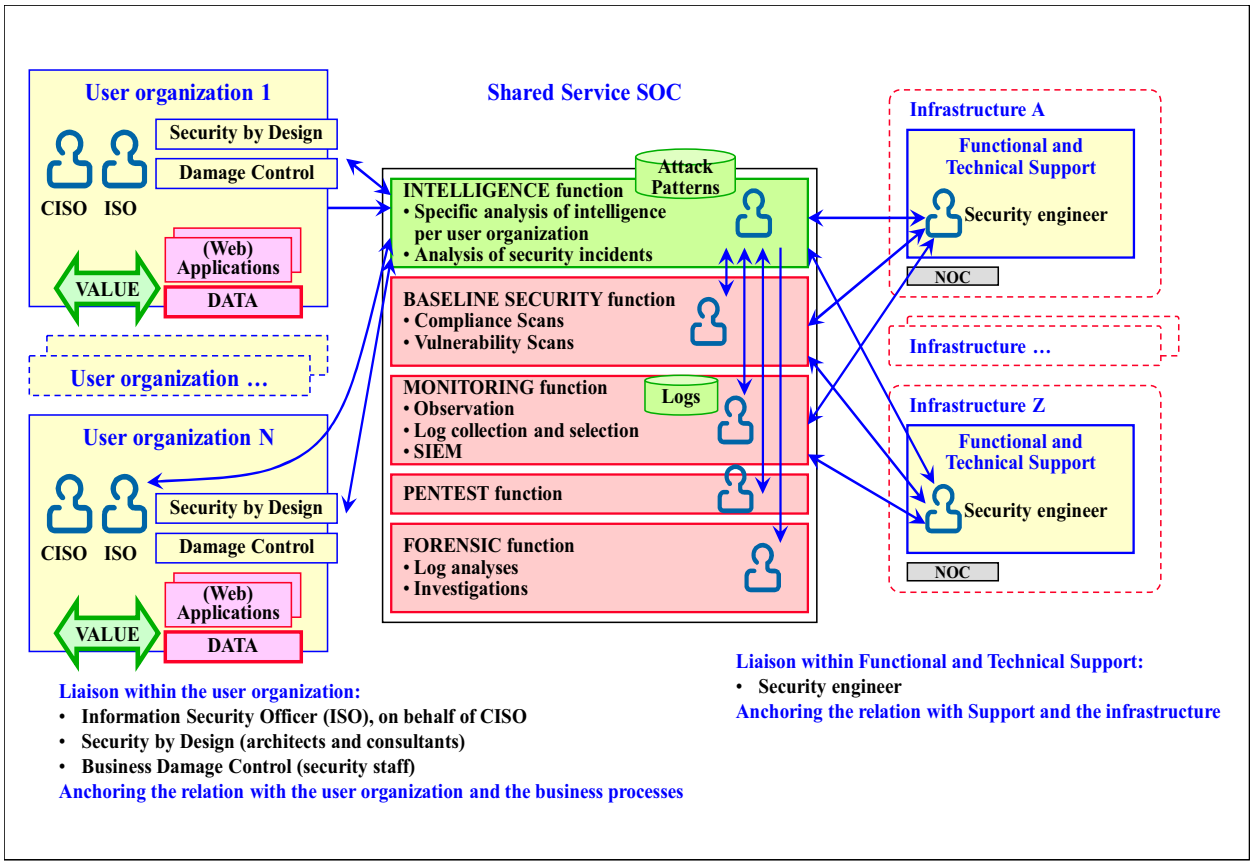

Figure 5. Centralized SOC with local liaisons

offer. So, the manager of the SOC must always expect to lose one or two of the most experienced penetration testers, and has to employ one or two juniors who need time to be educated and trained. If the manager wants a core team of four mid-level or senior penetration testers continuously, he or she must employ a group of seven.

5.1. Anchoring the SOC

Each of SOC's functions has inseparable relationships with functions within the user and IT organizations. In Figure 4, these relationships are shown.

The Intelligence function of the SOC maintains a close relationship with the user organization, since it has to focus on protecting against threats specific for this business, and the customer and user community. This task can only be performed with sufficient knowledge of the user organization, being aware of all relevant changes, and with close contact with the CISO, Information Security Officer (ISO), security staff, information managers, project leaders, architects, etc. Hence, there must be at least one analyst within the Intelligence function, acting as liaison for the user organization.

Three functions of the SOC, i.e. Intelligence, Baseline Security and Monitoring, need a close relationship with the engineers and staff of Functional and Technical Support within the IT organization. They must be aware of the changes affecting security, security incidents, release management, patch management, etc. and must give instructions about the hardening process, high priority and security patches, settings for security related parameters, logging and collecting logging information, etc. Moreover, they need to be authorized to access many sensitive parts of the network and systems to perform their investigations. At the very least, the SOC needs a liaison within the IT organization, in Figure 5 indicated as a specialized Security engineer. This engineer is the primary entry point for the SOC.

5.2. Providing security to multiple user and IT organizations

The third sub-question for this research is: '*How can a SOC provide adequate security services to mul-*

tiple user organizations and IT organizations?' The reason for asking this question is that skilled analysts are scarcely available, tooling for each SOC is expensive and tailoring and maintaining the tooling turns out to be an awkward and time-consuming process. Hence, the search for ways to let a SOC of one organization provide security services to another organization, which is beneficial for large companies with multiple divisions or a government with many governmental agencies. Exploiting the inseparable relationships, as explained above, Figure 5 shows an answer to this question.

In the case of supporting multiple organizations, the SOC has to implement dedicated communication lines at the business side. Within the Intelligence function of the SOC, there should be a dedicated liaison for each user organization, knowing the business and intimately interacting with the relevant actors within the business. The user organization performs the Business Impact Analyses (BIAs), Risk Analyses (RAs) and Privacy Impact Assessments (PIAs). So information about the requirements for confidentiality, integrity and availability are provided to the SOC, which can focus on the threats and vulnerabilities relevant to the particular business.

At the IT side, there is also a liaison required per IT organization. This liaison should be a person located between the support staff and engineers of this IT organization. This person is the local Security engineer, who is aware of all security related changes, security incidents, configurations, settings, and so on, within the IT organization. He or she gives such information to the SOC and passes guidance and instructions from the SOC to the support staff and engineers.

By appointing liaisons at the business and the IT side, the SOC will be able to ensure the inseparable relationships, vital to efficiently delivering the security services required.

6. Evaluation

Assuming this model is adopted by a country to protect e-government services for multiple agencies, a number of practical issues have to be solved. If, for example, the SOC operates for more than one Ministry, the individual ministerial responsibility is an issue. In the case of a severe incident, which minister has to submit to parliament – the minister responsible for the SOC or the minister who suffered the cyber-attack? Another point of discussion is funding, which is mainly an issue if a SOC is used to protect a chain crossing a number of agencies and private parties. There is a number of leads for further research in this area.

7. Conclusions

The primary recommendation is not to re-invent the wheel multiple times. It makes no sense to create tens of SOCs, knowing that there is only a very limited number of very skilled analysts available, and many SOCs struggle with implementing and tailoring (expensive) tooling in a meaningful way. Such problems can be solved by an increase of scale, e.g., by creating one SOC for an important chain. For a country, this may be one SOC for the large financial streams and e-governance, such as taxes, subsidies and pensions, one SOC for law enforcement, courts and penitentiary institutes, one SOC for the vital infrastructure, etc. Since the framework is focused on a SOC operating for multiple user and IT organizations, it allows for such a form of concentration.

8. Acknowledgment

We appreciate the close cooperation with many organizations and authorities. They have provided many insider details about the operational processes and have participated in the completion of this framework for a SOC. In addition, we want to thank the staff of VU University Amsterdam for their support in writing a graduate thesis about this subject.

9. References

[1] Bashar Matarneh, H., "World Financial Crisis and Cybercrime", 2011.

[2] EY, "Security Operations Centres against Cybercrime, Top 10 Considerations for Success", 2013.

[3] FOX IT, "Black Tulip, Report of the Investigation into the DigiNotar Certificate Authority Breach", 2012.

[4] Hoepman, J.-H., Jacobs, B., Vullers, P., "Privacy and Security Issues in e-Ticketing - Optimisation of Smart Card-based Attribute-proving", in V. Cortier, M. Ryan and V. Shmatikov (eds), Proceedings Workshop on Foundations of Security and Privacy, FCS-PrivMod 2010, Edinburgh, UK, 2010.

[5] HP Enterprise Security Business Whitepaper, "Building Successful Security operations Centre", 2011.

[6] IBM, "Strategy Considerations for Building a Security operations Centre", 2013.

[7] General of the Army Marc Watin-Augouard, Gendarmerie Nationale France, "Prospective Analysis on Trends in Cybercrime from 2011 to 2020", 2011.

[8] McAfee White Paper, "Creating and Maintaining a SOC, the Details behind Successful Security Operations Centres", 2011.

[9] Microsoft, “Simplified Implementation of the Microsoft Security Development Lifecycle”, 2010;
[10] National Cyber Security Centre (NCSC) Netherlands, “Cyber Security Assessment Netherlands”, 2013.
[11] Nohl, K., “Mifare security”, 24th Chaos Communication Congress, 2007.
[12] Reply Communication Valley, “Security Operation Centre”, 2011.
[13] RSA Technical Brief, “Building an Intelligence-driven Security Operations Centre”, 2013.
[14] Security & Defence Agenda (SDA), Belgium, “Cybersecurity: The Vexed Question of Global Rules”, 2012.
[15] Trustwave, “2013 Global Security Report”, 2013.
[16] US Intelligence Community, National Intelligence, “Information Sharing Strategy”, 2008.
[17] Yin, R.K., “Case Study Research Design and Methods”, 2009.