National Cyber Security Centre
Ministry of Security and Justice

Building a SOC: start small

Start simply, grow according to demand

Factsheet FS-2017-04 | version 1.0 | 15 November 2017

A Security Operations Centre (SOC) is an effective facility for monitoring business information security and digital threats. Establishing such a centre, however, requires investment of time, effort and resources. In order for a SOC to function successfully, it must keep pace in a controlled manner with the organisation's need for visibility and control of information security. Start small, share results with the organisation and build on a positive reception to these results to realise the next step in the development process. Ensure the planning, roadmap and implementation of a future SOC are realistic. Keep in mind that a SOC is a means and not an end in itself.

Background

Protecting and defending against digital attacks requires visibility and control of the digital infrastructure within your organisation and of all the events taking place within this. An increasingly common way to achieve this is to implement a Security Operations Centre (SOC).

Target audience

This factsheet is aimed at Information Security Officers in organisations that wish to begin monitoring business information security.

The following parties have contributed to this factsheet:

AlertTeam, the Tax and Customs Administration, the Ministry of Security and Justice, the Directorate-General for Public Works and Water Management, SSC-ICT and the Volksbank.

What are the challenges?

Effective operation of a SOC requires cooperation with many parts of the organisation since information is processed across the organisation as a whole. This means the establishment of a SOC is a daunting task, which brings a wide range of issues into play.[1] However, experts that can offer assistance in this regard are difficult to find, given that SOCs are a relatively new phenomenon. Building a SOC is also costly and time-consuming, and it can therefore be challenging to convince management teams of the value and necessity. This factsheet will help to address these challenges.

Building a SOC is mainly an organisational challenge, despite all the technology involved.

What is a SOC?

There is no set definition of what a SOC is, but practice shows that SOCs are most commonly tasked with security monitoring. This involves the centralised collection and correlation of log data from relevant applications and devices in the network, in order to identify any deviations that may have taken place. The collected log data can relate to a wide range of applications and devices – from intrusion detection systems, firewalls, web applications, Active Directory servers and anti-virus software to industrial control systems. This may involve any system able to supply information relevant to providing insight into the security or status of the network and the systems connected to it. When determining which type of information to collect, which systems to collect information from and which correlation method to use, the key is to focus on information relevant to the organisation rather than on what is considered customary to collect.[2]

A Security Information & Event Management (SIEM) system is a tool that forms an indispensable part of a SOC. SIEM systems are software products that are able to interpret log data from various sources and correlate it with cyber attacks and other security incidents taking place in and around the network.

In addition to information regarding systems and the network, a SOC also uses what is known as threat intelligence – information from external sources regarding vulnerabilities and threat information in the area of cyber security. This information can be used to assess events relating to systems and within the network.

[1] For an overview of aspects to consider when setting up a SOC, see http://rafeeqrehman.com/wp-content/uploads/2014/12/Building_SOC.pdf

[2] For background information, see http://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf

Simple monitoring as the starting point

Building a fully fledged SOC from scratch is a major challenge. A simpler approach is to start small and then build on this in a slow and controlled manner to create a fully fledged SOC. In order to achieve this, begin by having the IT administration team monitor log data from a select number of key infrastructure or middleware components, such as your firewall, a web server or your antivirus program. Target the monitoring on technical aspects initially, in order to confine the necessary interactions to the IT administration team. Focus on notifications highlighting a specific problem or on indicators of potential future issues. Report any findings to the IT service desk.

There is a wide range of software products available that enable monitoring of log files. Use a search engine or make your own enquiries to help you make your choice.

Build up experience with the monitoring, detection, registration and mitigation of incidents. Do not increase the number of systems to be monitored too soon. At the beginning, the main emphasis should be on gaining experience with the entire monitoring process rather than the monitoring itself. Ensure you have the right tools for registering incidents, generating periodic reports on this and recording any lessons learned. Arrange for staff tasked with the monitoring to participate in the appropriate meetings within the IT administration team and meetings relating to change management. This will leave them well prepared for any changes to the network.

When you set out, do not focus on building a SOC, but simply begin to gain insight into security based on the needs of your organisation. There is nothing wrong with finding at a later point that what you have created is in fact a SOC.

What is needed to be able to monitor security incidents?

In order to achieve adequate monitoring of information security, organisations will need to do more than simply check the log files of an antivirus program, firewall or similar. Before the monitoring structure within the IT administration team can be developed into a SOC, there are a number of measures that the organisation must put in place first.[3]

Information security policy

[3] For aditional information, see https://www.cip-overheid.nl/wp-content/uploads/2015/07/7-kritische-succesfactoren-voor-een-SOC.pdf

A key measure when building a SOC is having an information security policy that has been approved by the management. An information security policy describes the information security objectives of the organisation and the manner in which information security has been organised by it (who is responsible for what). The objectives set out in the information security policy can help to establish the areas that the SOC will focus on. The arrangements in the area of information security will identify the key stakeholders.

Overview of the application landscape

An overview of the application landscape provides insight into the information the organisation possesses and the manner in which the information is processed. Such an overview is key to an adequate and effective monitoring structure. This information is also an essential input for a sound risk assessment.

Results of recent risk assessments

Risk assessments help establish the consequences for the organisation when the availability, integrity or confidentiality of certain information is impacted. They also help determine which threats pose an unacceptable risk to the processing of information. This information clearly identifies the main focus areas for the SOC.

Another key input for a SOC are the results and outcomes of risk management. The risk management department is ideally positioned to answer the question of what the SOC should monitor. This does not necessarily cover office automation only. Any system or information processing is eligible for monitoring by the SOC if the risk assigned by the risk management department is sufficiently severe.

IT administration team

There is no doubt that a SOC will detect attacks and reveal vulnerabilities in the network. This will result in proposals for preventing attacks or enhancing security. Such proposals should not be taken up by the SOC itself, but are instead a matter for the IT administration team. Key aspects in this regard are a well-developed incident management procedure, a well-equipped IT service desk, adequate arrangements with the IT administration team on the priority of notifications made by the SOC and an appropriate mandate for the SOC.

Ownership of information systems

In most cases, the issues identified by a SOC can be tackled by the IT administration team. Nevertheless, incidents could arise that require decision-making at a strategic level. For this reason, each information system must have a manager as system owner to make such decisions. This concerns decisions that must be taken when a contingency plan is put into action, such as deciding whether to take an information system offline or on measures required to successfully cope with any offline time.

Development into a SOC

Using technology as a starting point is a good approach in order to initiate monitoring. However, for a SOC to become truly effective, it must be tied in with the business processes. Which are the key processes within the organisation, which information flows are essential to these and how could those information flows be disrupted? Putting processes at the centre of discussions makes it much easier to establish links with the various departments and the staff who work there. In order to succeed in establishing these links, it is necessary to ensure an appropriate development strategy for the SOC.

Knowledge and skills for SOC staff

Understanding business imperatives and monitoring the threats targeting the business goes beyond mere searches for technical issues in log files. A specific check can determine whether a system generates a certain error. But how do you establish whether a login is valid? Or whether any accessing, changing or deleting information is routine activity or the work of someone with malicious intent? An altogether different approach is needed when checking whether security has been breached. In such cases, this requires a different attitude and, in particular, a different way of thinking from staff. SOCs are a relatively new development, as a result of which skilled and above all experienced SOC staff are difficult to find. Therefore, start a new SOC with employees who have the right motivation and mind-set, and invest sufficiently in training.

Choosing whether to do it yourself or outsource

When implementing a SOC, an important decision early on is whether to outsource it.[4] The organisation may choose to set up and manage all the individual components of a SOC itself or outsource them to a third party. Each organisation will have its own specific needs, demands and challenges with regard to a SOC. Each option must be assessed in terms of flexibility, costs, available knowledge and personnel, etc. These specific needs and demands can only be met if the right decision is made between doing it yourself, outsourcing or perhaps a combination of both.

SOC services and products can be acquired from a large number of providers. Gain a better understanding of what is available on the market and what is involved in operating a SOC, by approaching several parties about the services they are able to provide. If the information that is processed by a SOC is sent outside the organisation, ensure compliance with the applicable legislation.

[4] See also https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-0788enw.pdf

Processes

The incident management procedures are among the key measures to put in place as they will help everyone to understand what is expected of them. Define types of incidents by distinguishing between levels of impact and establish which steps SOC staff should follow. Establish which staff members should be approached if an incident arises. For this purpose, select staff members with the appropriate responsibilities and mandate. Tell them that they may be approached in the event of an incident and what decisions they are expected to make. Establish the required options for scaling up or escalating matters and arrange this with the relevant responsible staff members. In other words, ensure expectations are managed appropriately within the organisation. Make arrangements for normal monitoring tasks within the SOC to be continued during an incident. Develop a communication plan and design processes so that the deployment and added value of the SOC can be measured.

Engaging with the business

A SOC must engage with the business in order to understand what is important to it. Liaise with the appropriate managers and system owners. Involve the risk management department in such discussions. The information security policy and the outcomes of risk assessment can help provide insight into threats and to prioritise these appropriately.

Come to clear agreements with the business regarding the manner and format in which the information for the SIEM system is to be provided. Use periodic reports to engage the organisation in the results achieved by the SOC.

Selecting an SIEM system

Although the majority of the challenges in building a SOC relate to organisational matters, there is also a key technology choice to be made – the selection of the SIEM system.[5] Many of these solutions have similar capabilities. The key differences are in the details, which means it is tricky to select the right system. A good decision is only possible once it is sufficiently clear whether a solution is able to address all the needs that exist within the organisation. A sensible approach, once all the organisation's needs have been established, is therefore to approach suppliers, visit trade fairs and, if possible, visit organisations that have already implemented a SIEM system. Ensure you consider this decision carefully. Once you have chosen a solution, it will be costly and labour-intensive to migrate to another solution at a later time. In addition to the capabilities of the SIEM system, also consider the installation and maintenance requirements and the knowledge the SOC staff will need to have.

[5] Gartner regularly publishes an overview of the maturity of SIEM systems: https://www.gartner.com/doc/reprints?id=1-3EG4GVX&ct=160810

Threat intelligence

A SIEM system will flag up a wide range of issues. To be able to assess those issues properly, the SIEM system and the SOC staff will need to be provided with accurate information and insights. Invest in the acquisition of threat intelligence that will be used to feed the SIEM system and ensure SOC staff have sufficient time to keep up-to-date with developments in the area of digital threats.

Impact on privacy

Information that is processed for the purposes of monitoring may include privacy-sensitive information. Together with your privacy officer, conduct a Privacy Impact Assessment (PIA) for all data collection activities that could include privacy-sensitive information. Investigate the options that the available SIEM systems offer in the area of privacy protection.

More responsibilities for a SOC

Various parties point to tasks other than monitoring that could be given to a SOC.[6,7] Although it is of course possible to accommodate the tasks of a range of employees (such as the performance of penetration tests and forensic IT investigations) within the same organisational structure, caution is advised when assigning additional tasks to staff tasked with monitoring. Do not use quiet times as a reason to increase their tasks. This carries the risk that the additional tasks will not be given sufficient attention in busy periods or during incidents. Use quiet times to critically review the security monitoring set-up, gain new knowledge, carry out drills and get up to speed with developments. Cyber criminals are continually on the lookout for new ways in which to carry out their attacks. Allow SOC staff to continually dedicate attention to this.

Developing the SOC further

One of the risks of allowing a SOC to grow too quickly is that the amount of information collected exceeds the processing capability of the SOC.[8] In addition to this, the IT service desk must be prepared for the number of notifications that a SOC will submit to them. Restrict the data that will actually be collected on the basis of the throughput capacity of the SOC and the IT service desk. Ensure that the expectations are clear by communicating these objectives clearly to the organisation. Discuss with the management team how the SOC and IT service desk can grow in a controlled manner.

Extension of a SOC will most likely result in an increase in the number of aspects to be monitored. Put differently, there will be an increase in the number of correlation rules used to

[6] See chapter 8 in https://www.jbisa.nl/download/?id=1770008
[7] See 'Soorten SOC' (Types of SOCs) chapter in https://www.pvib.nl/kenniscentrum/documenten/expertbrief-security-operations-center-een-inrichtingsadvies
[8] https://www.computable.nl/artikel/nieuws/security/5901142/250449/security-operations-centers-worden-overspoeld.html

determine whether an undesirable event or deviation has occurred. More rules means an increase in the maintenance required for these rules, since each change made to a system or the network might require a change to one or more rules. Ensure the SOC is prepared for this.

A SIEM system is able to handle large volumes of information in order to zoom in on relevant issues on the basis of smart, customised rules. For mature SOCs, this includes the standard technical checks as well as checks and matters that are closely linked with the day-to-day processes of the departments. A pitfall in this regard is that a SOC performs checks that, although helpful to a department, have little to do with information security. A SOC must remain watchful that its checks continue to serve its original objective and that it does not allow itself to become a big data department for the organisation as a whole.

In the event that the organisation has established a Computer Security Incident Response Team (CSIRT), allow the SOC to take part in this. The SOC is able to provide useful technical data that can help to trace the cause of an incidents and the origin of any attacks.

The maturity level of a SOC can be established with the help of the SOC-CMM[9] – the SOC Capability & Maturity Model. The principles in this model can also serve as the starting points for a roadmap or as a checklist for building a SOC.

Conclusion

A SOC is an effective facility for monitoring business information security and digital threats. Establishing such a centre, however, requires investment of time, effort and resources. In order for a SOC to function successfully, it must grow in controlled fashion along with the organisation's need for insight into and control of information security.[10] Start small, share results with the organisation and build on a positive reception to these results to realise the next step in the development process. Ensure the planning, roadmap and implementation of a future SOC are realistic. Keep in mind that a SOC is a means and not an end in itself.

[9] https://www.soc-cmm.com/
[10] For aditional information, see https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

Publication
Nationaal Cyber
Security Centrum (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (70) 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2017-04 | version 1.0 | 15 November 2017