Orange
Cyberdefense

The road to your own SOC

Critical steps you must consider when building your own SOC, regardless of the level of ambition.

Table of contents

© Orange Cyberdefense

Martin Sundqvist
Professional Services Manager
Orange Cyberdefense

Security Operations Center

In today's digital landscape, it is virtually impossible to stay one step ahead of complex cyber threats. If anyone wants to access your information, they will probably do so sooner or later. The threats in our digital world have risen dramatically and rapidly, where the approach of criminals is becoming increasingly advanced. Being able to detect and respond to carefully hidden and difficult-to-detect threats and try to predict them is therefore of utmost importance. The only thing the intruder needs to find is a weak spot, and the intrusion is a fact.

The advanced technical solutions and services that are developed and implemented by organizations and companies naturally provide some protection. Firewalls, antivirus software and Endpoint Detection and Response (EDR) tools can slow down the more obvious and identified threats. But at the same time it is easy to blindly stare at the technical tools and rely on their ability to prevent attacks. To ensure you have the capability required to respond to different types of incidents, you need to have a complete overview of your IT environment, close any security holes and adapt to new, possible threats. In addition, all safety efforts that are carried out should be analysed and measured so that you can develop and deepen your defense.

Authorities and organizations that have certain restrictions and requirements to follow, companies that run all or part of their business online or have some form of IP (Intellectual Property) should have an advanced and well-thought-out IT security management plan. Whether you choose to build full in-house functionality for security analysis and response processes internally or if you bring in external help from a trusted security partner.

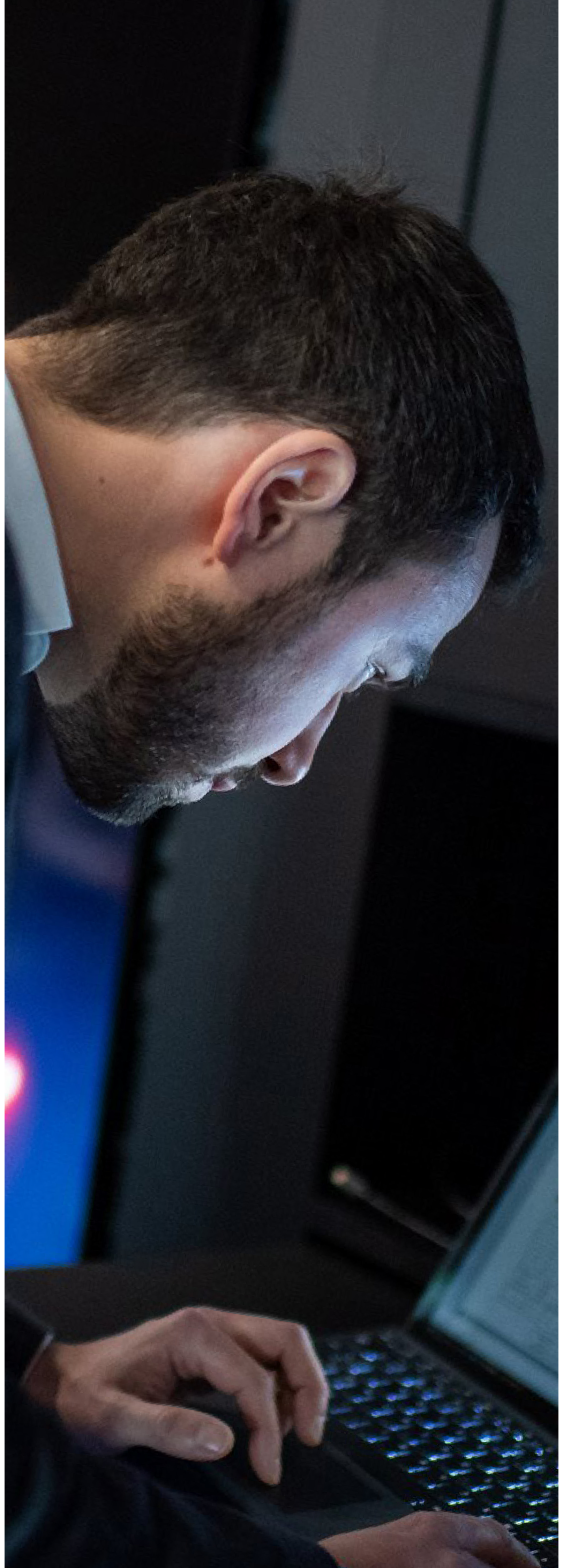
© Orange Cyberdefense

SOC - Security Operations Center

As a complement to the technology you invest in, more and more organizations are choosing to set up their own SOC (Security Operations Center). A SOC can be described as a unified security function including both human resources, advanced technical solutions that are used to detect intrusions, violations or attacks together with processes for safe and qualitative handling. It is a security team whose main task is to make different risk assessments in different infrastructure, IT and business systems of an organization. They should create a clear view of the vulnerabilities and detect and respond to potential attempts from outsiders who try to exploit known vulnerabilities. The SOC's task also includes reporting to the organization on vulnerabilities, monitoring the outside world, mapping the security situation and proposing measures. Depending on the organization's size and risk appetite, a SOC can be different in size and consist of anything from a couple up to a dozen SOC analysts.

This white paper aims to guide you in how to set up your own SOC. There are many important parts to keep in mind when setting up a SOC - no matter what level of ambition you choose. Therefore, here are the most important steps, our best tips along the way, what tools and technical equipment are needed and how you can best measure success within the SOC.

© Orange Cyberdefense



Why a SOC?

If you don't understand your security posture - then you also do not know what shortcomings you have. Could your business possibly be leaking information somewhere, has a malicious code been planted that you do not know? If you do not have complete control over your systems, your security situation and where information worthy of protection is located, you also do not know where a possible attack can take place. If, on the other hand, you have set up a SOC unit, you have a much greater chance of detecting and preventing any intrusion at an early stage. The importance of having a SOC and how advanced functionality it should contain, depends largely on the organization's requirements, risk appetite and how sensitive information should be protected.

If you do not actively have one or more people who, together with the technical solutions, work daily to look for potential threats or intrusions, it can take a long time before they are discovered. If you want to counteract any operational disruptions, due to different types of attacks, or if you have requirements to be able to follow-up and have traceability in your environments - for example, which people log into certain systems, then these tasks must be carried out by a SOC analyst.

The importance of human analysis

If you don't have a SOC in place, and you rely on then technology and systems you have invested to execute the full job, you lack the human capability to analyse events or incidents in more detail. The security products you have installed and configured will probably detect the events they are meant to detect, but they will fail where human evaluation is crucial. There could be events which require further investigation where technology cannot deliver. The function of a SOC analyst is to examine alarms, anomalies and incidents, assess the seriousness of these and respond if necessary. Having coherent reporting is critical for the effort to be effective and fruitful.

Increased awareness of cybersecurity (Radar Eco Report: Cybersecurity 2020)

In the latest global risk report from the World Economic Forum (World Economic Forum, Global Risk Report 2020, p.11, 63), cyberattacks on critical infrastructure are identified and valued as the fifth largest risk in companies, in a short-term risk perspective.

Nordic organizations have traditionally been regarded as less concerned about cybersecurity than in other regions/economies, which may be due to perceived social stability and confidence in the government. This is now changing and the Nordic countries have become more aware of the risks and threats that exist. Both the public and private sectors are now improving their capacity to meet cybersecurity requirements from a modern organization.

Stricter legislation that regulates the handling of data together with more frequent media reporting on security breaches and their consequences has pushed cybersecurity onto the agenda in the management rooms of most organizations and companies. In general, Radar's research indicates that the overall trend of perceived cybersecurity risk has a slightly rising level from year to year.

Regarding risk prevention and preventive cybersecurity measures, Radar states in its report that the result is very low. Nearly 50% of responding organizations "lack" direct measures to reduce risks and manage incidents.

The structure of a SOC

Orange Cyberdefense has many years of experience in building and managing SOC units. We believe in cybersecurity measures where technology meets people and processes. Building your own SOC means that you get the ability to adapt it to your specific requirements, allow you to work across organizational boundaries and get the most out of your security analysis platforms. Before an SOC is set up or implemented, it is important that the organization, together with any external actors, discuss the expectations of the SOC and then communicate with the entire organization what is being set up and the purpose of the SOC. When everything is then prepared and planned, the most important recommendation is to set up an SOC in stages. To have an effective SOC, technology, people and processes need to interact and work together in symbiosis.

Invest in the right technology

Investing in the right tools is a good start in security management. Technology is important and there are a number of innovative services and programs to support security management in a SOC. A large part of the technology development the recent years has been about SOC tools that automate and streamline. The technology should increasingly be able to analyze a security threat even deeper and help the analyst with better-compiled data and dependencies between events. The goal of the interaction between technology and man is to reduce the time from intrusion to action.

Gather people with the right skills

Having experienced and competent analysts on-site, who can analyze incoming data, detect incidents and have a solid ability to respond is a key to success in security management. No matter what technology you use, whether you invest in advanced and modern systems or work in more traditional tools, you will need people on-site who understand, manage and develop the solutions to meet the set requirements and the ever-changing threat landscape. It is also important that the SOC has constant staffing as the threat landscape is not limited to traditional working hours. The attacks take place from all corners of the world and during all hours of the day.

Set up relevant processes

In addition to the technology used and the people employed to analyze the data, you need to have effective processes in place to ensure that the right action is taken once an incident occurs. When something happens, it often goes quickly and action may be needed immediately. There should be incident management processes as well as processes on how to update your detection rules, whenever you find a new risk or before a new system is put into operation. When something new is implemented, you should always be able to answer the question: what are the risks and how can we get detection in place quickly?

Surveillance, detect and respond to the outside world

In short, these three tasks are part of a SOC analyst's everyday life. To daily, carefully monitor their surroundings, and not just focus on your environment, is of the utmost importance to be able to detect new threats or ongoing attacks at an early stage. To continuously develop your detection and response ability by constantly measuring what is being done, to contribute to more incidents being stopped before they have time to cause damage to the business.

Keep training

Training can have amazing effects on all the components of technology, people and processes. Today, there are several good simulation tools a SOC should use to train in detecting a threat, test the internal processes to be used in the event of an ongoing intrusion, and test the efficiency and handling of the tools you have access to.

Which tools are needed?

Which tools a SOC needs today depends largely on the organization's or company's business, risk appetite and resources. For a modern SOC unit, however, there are some basic tools that should be in place.

Log collection platform

The most basic thing a SOC needs, is a log collection platform which stores all the logs coming from different types of systems so that everything is available in one place. There, the SOC analysts can see what is happening on all affected servers and clients and quickly provide an overview.

Detection system

Today, there are different types of detection systems that can be applied to both networks and endpoints which can be very helpful for a SOC. They also contain Machine Learning (ML), which facilitates human work around the analysis.

Incident management system

All organizations that work with IT, technology and ticketing need a good integration of case management or some form of an incident management system. In that system all relevant incidents can be registered to get a comprehensive history. It also makes it easier to pass on activities within the organization, if something needs to be analysed in more detail.

Document management platform

It is also advantageous to have an access-protected platform for documentation, in the form of a wiki platform or perhaps part of an intranet, where you can, for example, describe the SOC's capabilities, collect detection patterns, instructions, etc.

Playbooks

Instructions on how different cases should be handled and in what order things should be done - before, during and after a security incident should always be documented in security playbooks. These can be built into any type of platform or system. By using clear security playbooks, the SOC can gain very good insight into its own process, and through this also create effective improvement routines.

Automation platform

A system that can automate parts of the SOC's work can be implemented when you have a clear picture of which threats exist. In such a platform, ready-made rules and use cases are built-in, so the proportion of incidents that need to be analyzed manually is minimized. You should also think about good access protection, as the data that is handled is sensitive and can contain personal data, even about your own staff.

Where to start

Once you have decided to set up your own SOC, many things need to be set in place. Many people get the feeling that they want to run for solutions right away, but there are several important steps to pass before you buy anything off the shelf.

Current situation analysis

To begin with, you should always analyse your current posture. Evaluate your resources, security maturity and the desired situation you aim for. The desired situation is key for both us to look at and for you as a business to keep in mind.

When we do a current situation analysis, we often work according to the Security Maturity Assessment. A measurement based on several issues concerning IT security, where we map the company's maturity in the area. Based on that we develop the necessary skills required and examine the shortfalls and ways to overcome them.

Update to the right technology

Map out what systems and technical solutions you have today, what you would need to invest in now and may need to invest in in the long run. Make a separate roadmap for the technology and take stock of what resources you have. All to ensure that you know what is needed to set-up a SOC.

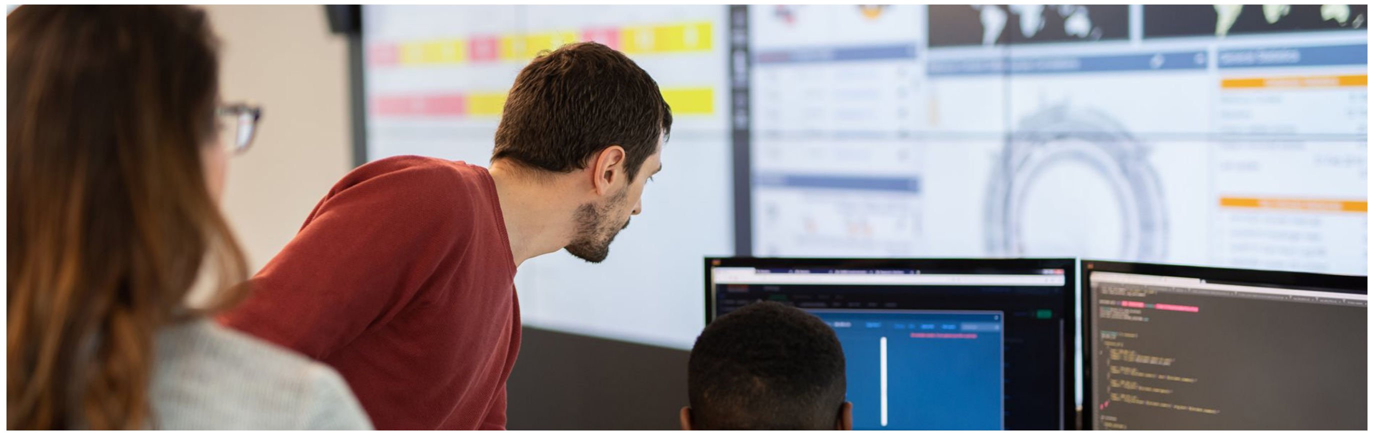
Hire the right people

It can be difficult to find SOC analysts with the right skills. Experienced analysts do not grow on trees and those who exist are incredibly sought after, thus expensive. We have extensive experience in developing role descriptions for SOC analysts and we are happy to contribute our knowledge, as it can be difficult to know exactly what such a role entail and what characteristics they should retain. Examples of properties are:

- Solid security interest
- Generalist in IT
- Analytical ability

If the person also has good knowledge of the organization, it is a plus, so hiring someone internally can simplify the process. What you should keep in mind is that even if the person has good insight into the company, it can take time to get acquainted with and learn how to work within a SOC.

A SOC can look and be built up in different ways but is usually based on the traditional division of roles: first line (tier 1) - second line (tier 2) - incident response. There must be one or a couple of people in the first stage who take care of incoming cases, detect and make an initial assessment of whether the alarm should be escalated or not. The second line makes a deeper analysis of the incident and the third line responds. In modern SOCs, these roles are not completely fixed, but it is advantageous that all analysts are able to rotate between the different roles. The most important thing is that there is always someone who has its eyes on the incoming case in the first place because the typical intruder tends to strike when the guards are looking elsewhere.



Define measured values

To be able to calculate your investments and justify the costs for the SOC, you must map out what it is you are going to measure. What should your SOC deliver, what incidents should you look at how the situation has improved since the SOC has come into place. If you don't know what to measure, it will be difficult to draw conclusions on the effectiveness of the investment and what you may need to adjust later. Measured values worth considering are:

- How many incidents are stopped with the tools you have purchased?
- How many cases does the SOC handle daily/weekly/monthly and how many of these are incidents?
- Based on use cases - measure how many own use cases the SOC has set-up, which can be an indication that the ability will be better.
- How good is your detection ability? This can be measured based on The Cyber Kill Chain model.[1]

Based on the analyses that are made, decide whether you can conclude if you can find other ways to detect threats or intrusions and continuously develop your detection and response ability.

Automate

There are several innovative and efficient tools for automating parts of the SOC's work. Automating processes and handling incidents is a practical and commonly used method in a modern SOC. However, there is a risk of automating too much and too early on the development of a SOC, when you are not yet familiar with the incidents which should be automated. Automation primarily alleviates the first line and reduces the number of incoming alarms. However, before such tools are implemented, the SOC should first identify and map out which threats exists. Automation can also be used to enrich data for the SOC analyst, so that more data is available when the alarm needs to be handled.

SOC Triad

The SOC Triad concept was introduced in the Gartner report "Applying Network-Centric Approaches for Threat Detection and Response" 2, published on March 18, 2019.

The research bases its theory on military methods to protect itself against attacks coming from several sources simultaneously. According to these researchers, a SOC must be built with the possibility of detection based on the same principle. In the case of the SOC, it is about SIEM/log, client and the network.

SIEM/UEBA provides the ability to collect and analyse logs generated by the IT infrastructure, applications and other security tools. Client detection provides the ability to capture execution, local connections, system changes, memory activities and other events from the client. Network-based detection (NTA, NFT and IDPS) is provided by the tools that are focused on capturing and/or analyzing network traffic.

Logs can provide the necessary visibility in higher layers. For example, they can provide visibility into what users are doing on the application layer. EDR (Endpoint Detection and Response) and logs can also alleviate problems related to encrypted network connections - a common cause of blind spots in network-centric technology. It is very important for a SOC to be able to answer the following questions: what did this account do before the alarm? What did it do after the alarm? Can we find out when it started?

The history of an event is generally found in three places: EDR (Endpoint Detection), NDR (Network Detection) and SIEM. EDR provides detailed information about the processes running on a "host" and interactions between them. NDR provides an overview of interactions between all devices in the network, regardless of whether EDR is running on them or not. Security teams configure SIEM to collect event log information from other systems.

Security teams that distribute the triad of NDR, EDR and SIEMs thus have the opportunity to answer a wider range of questions when dealing with an incident or chasing threats.

According to the researchers, your SOC triad significantly reduces the risk that an attacker will be able to work in your network long enough to achieve their goals.

[1] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[2] https://www.gartner.com/en/documents/3904768/applying-network-centric-approaches-for-threat-detection

© Orange Cyberdefense

The SOC of the future

No matter how much resources you have and how large the SOC you plan to build is, some of the most important parameters are to continuously develop your security management, monitor the outside world and review your abilities. Many companies are facing a major transformation with digitalization and need to take a holistic approach to their IT security management. The SOC acts like a spider in the web - but the entire organization must be included when it comes to the responsibility taken for IT security.

There is external help available

Parts of this document may sound overwhelming, but help is available. Either you choose to do some parts of your SOC work yourself and outsource the rest, or you choose to outsource all the work around the SOC to an external security provider who takes care of the alarms, when they go off. Another way is to outsource only the operation of certain services. Here is the opportunity to read more about services connected to the SOC Triad and how these can be set up: https://orangecyberdefense.com/global/services/detect-respond/

If you have questions or want guidance, do not hesitate to contact us at info@orangecyberdefense.com.

On our website www.orangecyberdefense.com there are also several blogs and more information about how to improve your security management.

© Orange Cyberdefense

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Our organization retains a 25+ year track record in information security, 250+ researchers and analysts 17 SOCs, 11 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense has built close partnerships with numerous industry-leading technology vendors. We wrap elite cybersecurity talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio.

At Orange Cyberdefense we embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. Their competence, passion and motivation to progress and develop in an industry that is evolving so rapidly.

We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our customers to focus on what matters most, and actively contribute to the cybersecurity community.

Our experts regularly publish white papers, articles and tools on cybersecurity which are widely recognized and used throughout the industry and featured at global conferences including, Infosec, RSA, 44Con, BlackHat and DefCon.