Whitepaper

SOC maturity & capability

Prepared by:
Katy Winterborn, Managing Consultant

Table of contents

1. Introduction

Security is a high priority for most organisations. A string of high priority breaches in big multinational companies has brought home the threat that all organisations face in the modern world.

As a result, a growing number of companies are considering how to best protect themselves and reduce the impact of a breach. It is generally considered best practice to assume that it is no longer a matter of “if” [a breach will occur] — it is a matter of “when” [1].

While good security and security assessments can go a long way towards preventing incidents, adversary tactics and tools are constantly improving and the use of advanced malware, such as in the WannaCry attack [2] shows that not all incidents can be predicted ahead of time.

Therefore, companies are turning towards a more reactive capability and this can be provided by a Security Operations Centre (SOC). This paper aims to give an overview of a SOC and its capabilities, describing the roles and responsibilities of a SOC along with some of the considerations and benchmarks that a mature and capable SOC might utilise. It will also consider whether a SOC should be internal or outsourced along with some of the questions that it may be useful to ask of the SOC in order to gain assurance that it is operating at the required level.

It is no longer a matter of “if” [a breach will occur] — it is a matter of “when”.

1.1 What is a SOC?

A SOC is responsible for monitoring the networks of an organisation for threats, attacks and breaches and bringing them to the attention of the relevant parties so that they can be contained and eradicated as quickly as possible.

A good definition of a SOC is given in [3], 'a SOC functions as a team of skilled people operating with defined processes and supported by integrated security intelligence technologies'.

One problem with setting up and running a SOC is that good security often produces no visible effect. After all, a sign that security is working is that no breaches occur. A blog by Komand [4] gives the best attitude towards a SOC: 'think of them as the fire department: while there may not be a fire to fight every day, that doesn't mean you don't need a fire department. The same goes for a SOC'. It is therefore important to understand that, while an attack may not happen today, that does not mean the SOC will not be required tomorrow.

On the reverse end of the spectrum are the 'unknown unknowns'. These are attacks that may be ongoing but remain undetected due to a lack of intelligence or because the attacker is advanced and has sophisticated techniques to remain undetected. Therefore, care must be taken to ensure continual growth and learning within a SOC with the associated investment in order to have the best chance of detecting this type of threat.

1.2 SOC roles

Day-to-day activities in a SOC will consist of monitoring alerts, investigating them in more depth and communicating with customers or other team members.

A networking world article [5] describes the overall aim of the SOC as working hard to manage the known and existing threats while keeping up with emerging risks and issues. All of this while attempting to keep aligned with the customer's needs and risk tolerance level'.

It is important to keep in mind the reasoning behind creating a SOC. They are often a cog in a much larger wheel and while finding the next big breach is exciting, the main aim is to serve the business in some way. The overall objective can be thought of as follows: 'maintaining business continuity is the most important responsibility entrusted to the SOC team' [6].

The SOC, along with other teams will be charged with protecting the business and 'from a security perspective, functionality and data are the principal objects to protect' [3]. This should be kept at the forefront of all decisions about what a SOC will and won't do.

1.3 Building a SOC

With the SOC's role firmly in mind, the next step is to actually consider how to build a SOC. Firstly, it is important to actually decide what the SOC will do and how that aligns with the business by 'clearly defining a strategy that incorporates business-specific goals from various departments as well as input and support from executives' [7].

It is also necessary to decide right from the offset who the SOC customers are, what the risk tolerance level is, what the highest priority assets to protect are and how to gain the support of senior level staff in order to enable the SOC mission.

Although this should be considered at the start, it is not a onetime activity. 'A successful SOC will undergo some transformations during its lifetime' [8] and so continued growth and change should be anticipated and planned for. It is important to acknowledge that existing controls 'become less effective over time as attackers find new and complex ways to bypass controls' [9]. As a result, the SOC will need to change and adapt in order to meet a new generation of threats.

1.4 People, processes & technology

A whitepaper by SANS Institute [10] describes a SOC as the 'collaboration and communication among multiple functions (people), disparate security products (technology), and varying processes and procedures (processes)'. These three components form the core of a good SOC and are consistent through all articles and discussions about building and maintaining a SOC.

All the components will need to be considered and balanced as they work together and missing one will leave a gap in detection capability. It is often the case that, when setting up a SOC, buyers can be seduced by a shiny technology product that promises to do everything. However, without the appropriate people and processes this will not offer the appropriate protection. As noted in the NCSC guidance on what to look for in a SOC [8], 'it is vital to establish the basics before attempting advanced analytics', time should be taken to establish a good core before anything else.

Another way of describing it is 'at the core of a successful SOC is a strong foundation for operational excellence driven by well-designed and executed processes, strong governance, capable individuals and a constant drive for continuous improvement to stay ahead of the cyber adversaries' [1].

1.5 Relationship with customers

All SOCs, whether internal or provided by a Managed Security Service (MSS) will have a customer to report to. It is their responsibility to respond to customer needs and protect their assets.

A good relationship with the customer is paramount when investigating and responding to incidents. However, it is important to note that notification of a breach is bad news for a customer and creates problems they need to deal with. It may mean critical services have to be offline for a period of time or data has to be restored from backups, while they are trying to maintain their day job. As NCSC highlights in their guidelines [8] ‘don’t assume your business wants to hear what the SOC finds’.

2. People

One of the most critical aspects to consider in any SOC is the people. The human element is often underappreciated but alerts are meaningless unless they can be interpreted and turned into actionable intelligence and then responded to. This is where the people working in a SOC come in.

Hiring and retaining the right people is often a challenge. This is because the qualities and skill set that describe a good analyst are hard to quantify and do not easily translate to a CV or job description.

The skill set for cyber roles is not easily written down and isn't necessarily obvious. It is often described as 'you just know the right person' by those responsible for hiring analysts. Analysts require curiosity and the ability to notice connections and patterns in large volumes of data. In addition, there will be an element of shift work if the SOC needs to be staffed 24/7, and even for roles that are not shift based, there will most likely be on call requirements.

According to Hewlett Packard [11] 'in order to staff a sustainable 24/7 SOC, a minimum of ten analysts are required. The shift schedule that best fits this staffing model leverages four shifts, each working 12 hours at a time. A minimum of two analysts should be on schedule at all times. Additionally, two of the more experienced analysts (commonly referred to as level two analysts) work an overlapping 8x5 shift and are available to cover shifts for planned and unplanned absences'.

There is a skills shortage globally in the cyber security industry and this is a problem within the SOC industry as well. As noted on the Digital Guardian [7] 'many security leaders are shifting their focus more on the human element than the technology element to assess and mitigate threats directly rather than rely on a script' and 'while technology systems such as firewalls or IPS may prevent basic attacks, human analysis is required to put major incidents to rest'.

Though the human element is a vital component of a successful SOC, when scripts are used effectively they can save time by automating repetitive tasks and freeing up analysts to focus on the more complex areas. As noted by Hewlett Packard [11], 'the number one issue facing security operations at organisations is finding the resources needed to run the business. Often, optimal staffing is not achievable'.

As highlighted in in a blog by Komand [12], 'one of the best ways to ensure that your people, processes and tools are all working together like a well-oiled machine is to implement security automation and orchestration'.

This is summarised well in an Infosecurity Magazine article on best practices for SOCs [13]. It makes the distinction between routine tasks and those requiring a decision to be made: 'if there is no judgment to be made, you don't need a human analyst – you need to automate'. This is vital as analysts can easily get stuck in tasks that take a human a long time but need to be done. The article goes on further to state that 'utilising technology to automate data collection and to perform analysis will enable SOC teams to effectively focus on the tasks where humans are essential'.

As well as analyst roles, effective leadership, both in the day-to-day management and at a senior level are critical for a mature and successful SOC. 'Each member of the team must be fully aware of both the mission and the strategy of the SOC; therefore, an effective leadership has an enormous impact' [14].

2.1 Analysts & technical staff

The majority of staff within a SOC will be analysts and technical staff. These will be the individuals responding to alerts, raising tickets and monitoring the traffic flowing into the SOC. The exact nature of analyst roles will vary between SOCs but at a high level they can be categorised in the following three areas:

Tier one analyst

The tier one analyst is the most junior analyst position and tends to consist mainly of graduates or those new to the cyber security industry. This role will normally involve responding to customer queries or notifications of alerts and deciding the appropriate course of action. Typically, the role will involve shift work as a SOC will normally provide a 24/7 coverage model.

Tier two analyst

For a SOC analyst the next stage of career progression is often to a tier two analyst. This role involves taking on tickets and cases that are more challenging than a tier one analyst is able to handle. A tier two analyst will typically have worked as a tier one analyst for a number of years and will have had exposure to the most common types of cases. They will also be experienced at handling most types of incident.

A tier two analyst may also cover a shift lead role. According to Hewlett Packard [11] 'a SOC shift lead role provides senior experience and accountability during a shift and shift turnover. Shift leads also ensure operational tasks are completed by priority'.

Subject Matter Expert (SME)

An SME will typically be the most experienced technical member of the team and will have specialist skills in an area. The specific specialisms at this level will vary, depending on the needs of the SOC, but may include reverse engineering and malware analysis, threat intelligence, hunters, SIEM engineers and incident response.

2.2 Management

Overall responsibility for the SOC will fall on the SOC manager, who will act as a final point of escalation for issues other SOC members aren't able to handle. In addition, this role will involve line management and support to the rest of the team, along with planning future growth and technologies to invest in.

An important quality for SOC managers is that they trust their staff and it is vital that this relationship is two way. This is because often the SOC manager will not be technical, but will need to make decisions based on technical information. This means they need to rely on the data passed from the analyst level and the key facts gained from it in order to make decisions.

2.3 Senior/board level support

An often underrated, but vital element of the SOC success is support from senior management, particularly at a board level. Without this support the SOC will struggle with growth and fulfilling their mission. Senior level support will show that the company values security at the highest level and gives the SOC authority to carry out investigations.

A blog by Komand [12] summarises the vital role that senior support has by firstly in defining the mission of the SOC: 'the CISO (or CIO) should be the one to put together the strategy, programs, policies and procedures to protect the organisation's digital assets, from information to infrastructure and more'. But also 'your C-level security representative should focus on clearly communicating the business case for security, and on developing a complete strategy that covers prevention, detection and response'.

2.4 Training & progression

As mentioned previously, finding the right staff is a difficult challenge and there is a skills shortage in the cyber security industry. Once the right people are in place retaining them is important, so it is vital to have a roadmap for training and progression.

In the first instance, a good training programme for novices helps to attract the right talent and ensures they have the skills and confidence for the role they are in. Training also helps staff feel that they are valued and can reduce stress levels as people feel better prepared for the challenges they may face.

A roadmap for progression also aids staff in feeling they have a future with the company and shows what their future role may look like and how to get there. With this in place staff can target their training and identify skills and weaknesses as well as identify where they are on a typical timeline.

As noted in a blog published on Cybrary [9] 'investment can be thought of as money and expertise'. Therefore, building the expertise of the SOC and retaining those skills is critical.

3. Processes

Having the right people in place is important for a SOC, but another important aspect is that those people know what to do and can assess how well it is being done. In order to achieve this, well-defined and measurable processes must be put in place to ensure that the SOC is working effectively.

According to a whitepaper by SANS Institute [10] 'to achieve efficient incident handling, the SOC must avoid bottlenecks in the IR process that moves incidents through tier one, into tier two and finally through tier three. Bottlenecks can occur due to too much "white noise," alerts of little consequence or false-positives that lead to analyst "alert fatigue".' This is a very real risk if processes are not defined and adhered to. In addition, when creating processes they must be realistic and serve the business while ensuring the analyst can achieve the goal. As stated in a publication by Ernst & Young [1] 'a SOC also needs to create processes with enough breadth and depth to sufficiently address the universe of possible incident scenarios and provide detailed guidance for response'.

According to an eBook by Alien Vault [6], the key processes are event classification and triage, prioritisation and analysis, remediation and recovery as well as assessment and audit. Each of these areas must be defined and documented, this is particularly important for tier one analysts, who may lack experience, so the steps to be taken in each stage are obvious. This is summarised well as 'a structured process is meant for enabling consistent operation and repeatable outcomes' [9] but also it should be noted that without the appropriate frameworks a SOC may be unable to act on intelligence as 'without policies and standards, the SOC has no authority to take action in response to findings' [1].

Legal protection and compliance are other key areas that are aided by processes and documentation. A blog published on Cybrary noted [9] 'creation of a SOC governance and operating model helps the organisation and SOC team to achieve accountability, guide communication and manage timely interactions with involved functions such as IT, IR, HR, legal, compliance and others'.

McAffee have produced a whitepaper on creating and maintaining a SOC [15] that details some of the documentation and processes that need to be created. The paper suggests creating a SOC manual that formally documents each of the mission, charter, objectives, responsibilities and operational hours as well as the following procedures:

- Monitoring procedure.
- Notification procedure (email, mobile, home, chat, etc.).
- Notification and escalation processes.
- Transition of daily SOC services.
- Shift logging procedures.

- Incident logging procedures.
- Compliance monitoring procedure.
- Report development procedure.
- Dashboard creation procedure.
- Incident investigation procedures.

3.1 ITIL/COBIT

Assessing the success of a SOC is a difficult task as more successful defensive technologies result in fewer successful attacks and this means a secure environment is one in which a SOC has nothing to see. It is also very difficult to measure whether no alerts are raised because there is nothing there or if compromises are being missed.

To bridge this gap, existing models have been used to assess where a SOC succeeds and where it needs to improve, specifically the most commonly used are IT Infrastructure (ITIL) and Control Objectives for Information and Related Technologies (COBIT).

ITIL is a series of documents detailing processes and procedures that align business needs with IT services. The COBIT is a good practice framework which defines a generic set of processes that can be used to measure IT implementations. In the case of a SOC, the COBIT maturity model section is often referenced.

3.2 KPIs/SLAs

Key Performance Indicators (KPIs) are a series of measurements that are agreed upon to assess the performance of a particular activity. Well-chosen KPIs can act as a metric to determine whether or not a SOC is operating at the required level.

Service Level Agreements (SLAs) are official commitments that a company must adhere to with a particular customer. Most often, they relate to acceptable downtime of a piece of equipment, but can also relate to response and communication times.

The main difference between a KPI and an SLA is that KPIs indicate how well a given activity is performed and areas for improvement. SLAs are mandatory and represent an agreement between client and vendor.

A blog published on Cybrary [9] highlights the fact that ‘documentation of Service Level Agreements, processes and chain of authority helps minimise any uncertainty and chaos during emergency high-impact actions’.

3.3 Responding to incidents

Once an incident has been identified and confirmed, the responsibility for handling recovery is passed over to the relevant response teams. It is possible that this may be an element of the SOC, probably a speciality that a subject matter expert may possess, but it may also be an external team.

The responsibilities and skillset of a response team differ from that of the core SOC. This is because they will need forensics skills and knowledge of how to contain an incident alongside decision making skills about whether machines should be wiped, whether data is recoverable and the ability to work and make decisions quickly. ‘There are a number of decisions to make when investigating an incident, particularly whether your organisation is more interested in recovering from the damage vs. investigating it as a crime’ [6].

The core SOC will work closely with the response team and to this end, having the necessary procedures in place will facilitate the work. Information such as machine details; any indicators of compromise; what may be known about an infection, including any threat intelligence, need to be accessible in a known format. This ensures the response team don’t waste valuable time by trying to establish something that is already know or obtain important data.

3.4 Metrics

Metrics allow a SOC to measure objectively how they are performing against a defined set of criteria.

An article by RSA [16] suggests that SOC metrics can be measured by how quickly incidents are identified, addressed and handled. This will give customers confidence in how the SOC is providing value as well as data for business cases on requirements for more staff or new technologies.

3.5 Use cases

Every SOC, whether internal or external, will have a customer with a set of priorities that they are most concerned about. In addition, the SOC has limited resources and cannot possibly guarantee that every aspect of a network will be analysed in detail or every signature from every signature set will get examined.

To this end, the SOC needs to understand the top concerns of the customers in order to ensure analysis effort is in the right areas and signatures are tuned towards areas of concern. A common way of doing this is via use case analysis. This will normally happen in a workshop type environment where the SOC and client representatives will detail the scenarios of highest concern to the customer.

‘An inability to prioritise efforts in your SOC results in an overall low capability and maturity - it is difficult and costly to protect everything. Successful SOCs utilise a risk-based approach that results in clear priorities and targeted focus’ [11].

3.6 Analyst procedures

In order for a SOC to run smoothly, it is important that everyone working there knows how to respond to a given situation and what information needs to be recorded. This is done via written procedures in an analyst playbook.

This will detail information such as what information needs reporting in tickets, when and how to escalate a case, what happens at the start and end of shifts and what information needs to be passed across when handing over.

As well as ensuring consistency, this gives an analyst confidence in what they are doing, speeds up the response to tickets and incidents as well as giving a measurable metric in how well these procedures are adhered to.

‘Defining repeatable incident triage and investigation processes standardises the actions a SOC analyst takes and ensures no important tasks fall through the cracks’ [10]. This is according to SANS institute in a whitepaper on building a world class SOC.

An eBook by Alien Vault [6] makes two key points in this area, firstly comparing analyst procedures to a more safety critical area of flying: ‘one of the most valuable tools an airline pilot has at his disposal is the simplest one. A checklist. The checklist enumerates every single thing that must be done in order to maintain safety, avoid risk and protect valuable lives’. It also ensures that everything is documented and means all the information necessary for auditing and compliance is readily available.

3.7 Other framework

As well as ITIL and COBIT, there are other frameworks that can be utilised. For example, ‘one of the most frequently used incident response process models is the DOE/CIAC model, which consists of six stages: preparation, identification, containment, eradication, recovery and lessons learned’ [10]. This was the US department of energy’s Computer Incident Advisory Capability (CIAC) and the documentation can be found on the Computer Security Incident Response Team’s (CSIRTs) website [17] as ‘CIAC Incident Reporting Procedures’. More recently, focus appears to have shifted to the NIST Computer Security Incident Handling Guide [18] which was published in 2012. It contains the same details around incident handling, but also adds sections that discusses setting up the appropriate team and information sharing.

In addition, a SOC needs to understand how it will perform under pressure and in the case of a high profile incident. This may not be a frequent occurrence and may have never happened (particularly if the SOC is fairly new). One solution to this is to run exercises to test the SOC in order to 'help the team to speed up their process under pressured conditions and attain maximum efficiency' [19]. NCC Group's SOCAlive (detailed further in section four) can be used to assist with this. Red teams can also be engaged for this purpose, providing they have the capability to generate attacks at differing levels of sophistication.

4. Technology

The third component of a successful SOC is the technology utilised and how effective it is. Although the danger of over reliance on technology is often highlighted, it is also true that a SOC cannot function without the right technology in place.

Different SOCs will have varying requirements. Solutions can range from high end technologies that are extremely complex to implement and require high levels of investment, to open source tools which need minimal setup.

When looking at appropriate technology solutions for a SOC, it is vital to note that 'the principle behind choosing SOC technology should be that technology should work for people and best processes, not vice versa' [9]. Though there are vast differences in the complexity and capability of solutions available, a few key pieces of technology will often be utilised in a SOC.

4.1 SIEM

A Security Information and Event Management System (SIEM) solution is arguably the most important piece of equipment a SOC can have. It is used for the aggregation of data from multiple sources and sensors and allows analysts to have a single view on the data in order to correlate patterns, investigate incidents or look for trends.

The actual sources that feed into the SIEM solution will differ depending on what is deployed on the network to be monitored, but may include log data, intrusion detection data, general network event data etc.

Note, however, as highlighted in the NCSC guidelines [8] on criteria for a SOC, 'SIEMs are not a panacea' they need tuning in order to provide useful information alongside skilled analysts to interpret the information, in order to assess the tuning of it and 'review regularly which SIEM content is providing benefit, and use stats to justify its existence'.

4.2 Dashboard

Most SOCs will have a visual system for representing what is happening at any given moment. This may display information such as system health, total number of alerts, average time to respond and/or close tickets as well as things like live news feeds, which may help predict attacks ahead of time or add context to ongoing incidents.

4.3 Ticketing system

A SOC, whether internal or external, will nearly always have an end customer to report incidents to and that needs visibility of the progress of an incident. This will be provided by the ticketing system, which allows the analyst to open a ticket and give details of an incident to the customer including relevant information such as affected hosts and any early information. The ticket can be updated with any new information or insights as the investigation progresses and closed once everything is resolved.

A ticketing system is valuable as it ensures nothing is lost and provides a storyline of what was investigated and when. It also provides insight and reassurance to the customer and can serve as a record of previous investigations. This can enable future work to be completed at a much quicker pace, as well as potentially feeding into threat intelligence systems. As noted in an eBook by Alien Vault [6], 'speed is a priority (but not at the expense of doing things properly)'.

4.4 Automated assessment tool

It is hard to objectively measure the performance of a SOC without known, repeatable attacks, and these are unlikely to happen in the wild, particularly for more sophisticated threats.

While there are a number of ways to assess the performance of a SOC under different scenarios from a purely technical perspective, one useful piece of software is an automated assessment tool, which will be discussed further in section five.

One example of this type of software is SOCAlive from NCC Group. It will 'automatically simulate the malicious activity of a Remote Access Trojan (RAT), controlled by a sophisticated threat actor, attempting to exfiltrate data' [20]. Run as a managed service it will start off very quietly and become noisier over time to assess at which point a SOC detects the activity to establish a baseline for performance [21].

4.5 Asset register

An asset register is an often overlooked, but it is an extremely useful addition to a SOCs technology suite. It provides a record of everything that should be monitored, what it is and relevant details about the asset.

The value of this is that when investigating an incident it provides vital information around what is potentially under attack and if that behavior makes sense, either as an attack against that system or if it can be explained as normal behavior.

As stated in a publication by Ernst & Young [1], 'to manage events that align to business priorities and assess the true risk or impact to the organisation, the SOC needs a well-maintained enterprise asset management system (which includes criticality of supported business processes)'.

4.6 Document store

There are many other pieces of technology that may be useful, one that may be included is an online document store. This ensures that analysts have access to the most up-to-date information and are not referring to out-of-date documents.

4.7 Bespoke vs off the shelf

A vital question to answer is whether products should be bespoke and tailored to fit the exact needs of the SOC or if off the shelf products will suffice.

Bespoke offers the advantage that the solution will provide exactly what the SOC requires and analysts can feed into the requirements process. However, there is a lag while the software is developed and it can often be more costly and may involve reinventing the wheel.

Off the shelf software is not tailored in the same way and so may not have the exact features an analyst may desire. However, it will have been designed to meet the needs of a customer base (it may or may not be SOC specific) and will therefore have had some form of requirements capture and so should meet most needs. In addition, it is often cheaper and available immediately.

5. Other considerations

People, processes and technology are the three main areas most papers will discuss when talking about SOC maturity. However, there are a number of miscellaneous considerations that do not naturally fit into these categories. These will be discussed below.

5.1 Environment

Due to the nature of a SOC's work, it will come into contact with sensitive information, which may include confidential information that is not to be shared widely. This may be due to the fact that someone within a company is under investigation or it is material of a disturbing nature.

Alongside this, the SOC will work as a team and may need to share information or discuss an investigation rapidly. As noted in a blog published on Cybrary [9], 'as SOC analysts work in a team (rarely in isolation), their performance tends to be effective when in physical proximity to each other'.

With this in mind, the SOC will need a segregated area from which to work. This should be access controlled and separated from the rest of the company in order to facilitate confidentiality and team working.

5.2 MSSP vs internal

Another important consideration is whether a SOC should be stood up internally or outsourced to a Managed Security Services Provider (MSSP).

Both have a different set of pros and cons and choosing the right option will depend on the individual needs of the organisation. An internal SOC will have quick and easy access to systems in case of a compromise, access to the people who know and manage the systems in order to ask questions and will be solely focused on protecting their own company. However, an MSSP will already have experienced staff and will save the requirement of recruiting a new team. A lot of the technological requirements will also be outsourced which will enable savings on the investment made and on the decision about what solution to use. Additionally, an MSSP will have a wider view on the industry and may have advanced knowledge of attacks and can correlate events from multiple sources that may help detect malicious activity sooner.

When considering if an internal SOC can provide the required service, the following question from an eBook prepared by Alien Vault [6] should be asked - 'How confident are you that your team has the resources and skilled staff to detect, contain and respond to a data breach? If your team's resources are concentrated on other priorities, it may be wise to leverage an MSSP to manage your SOC'.

5.3 Hunting

Intrusion detection and network monitoring are usually done using indicators of ‘known bad’ activity. This will involve looking for known bad IP addresses, email addresses, indicators of compromise or other data that can be gained from threat intelligence sources.

However, this kind of approach will not find new and emerging threats. This requires a type of activity known as ‘hunting’. Hunting involves looking at all the data available and searching for anomalies or other indicators that something is wrong. For example, it may include looking for abnormally large file transfers or out of hours activity. Often, it will mean obtaining a baseline for what normal behavior looks like and then looking for deviations from this norm. As noted in a whitepaper by SANS Institute [10] ‘the ability to create a baseline of activity for users, applications, infrastructure, network and other systems, establishing what normal looks like, is one advantage of aggregated data collected from various enterprise sources’.

Although hunting will find new and previously unknown attacks and compromises, the downside is that there is a much higher false positive rate and it involves interaction with other departments to explain anomalies or investigate further. The success of hunting style investigations very much depends on the customer tolerance level for false positives and relationships with other parties.

Legal issues also need to be taken into account while hunting. Data protection and privacy laws mean that personal data must be handled appropriately, although this is a concern generically through any defensive and investigative operations. Extra care also needs to be taken while hunting as there is often no justification for delving into user data as there would be with, for example, a signature hit.

5.4 Exercises & assessment

It is very difficult to benchmark how well a SOC is performing without a predictable, known attack to measure detection rates against. As mentioned in the ‘technology section’, this can be achieved through the use of an automated attack tool. However, this will typically mimic a malware infection or post infection behavior and in order to assess initial attack stages or more human driven interactions, red teaming will often be used.

Traditionally, a blue team is defensive in nature and a SOC would be classed as a blue team. A red team is the opposite, a purely offensive team whose goal is to hit certain flags within a network without being detected. They will normally keep detailed notes around how compromises occur and, unlike a traditional penetration test, try and penetrate as deeply into a network as possible rather than reporting on a breadth of issues [22] (note that this is referring to the cyber aspects of red teaming rather than the physical security aspects). This allows debriefing with the SOC to ascertain what was detected and when as well as what was missed and why.

Purple teaming [23] is a new concept within the cyber security industry and refers to a mixing of red and blue teams. As cyber offence and defence can't really take place in isolation, in order to succeed at one, it is a requirement to understand the other and therefore merging the two makes sense. In order to defend an asset, the specialist knowledge from a red team in how they would attack can help an organisation to improve defences and detection.

5.5 NOC vs SOC

Network Operations Centre (NOC) and SOC are two different areas that have a very close relationship and may be combined.

The NOC is responsible for network uptime and maintaining the devices on it. This can often feed into the SOC as it can explain behaviour, quickly provide an asset list and moving staff between the SOC and NOC can provide valuable cross skilling.

5.6 Additional responsibilities

While the SOCs main responsibility is monitoring network traffic and responding to incidents, they are often tasked with additional responsibilities.

One area that may fall under the remit of the SOC is vulnerability assessment. Most commonly this falls under a penetration testing team instead, but within a SOC it can give an indication of weaknesses or areas an attacker may choose to target.

In addition, it may be that the SOC is occasionally quiet and analysts will be tasked with administration and operational tasks. The decision to do this needs to balance the effect of putting too much pressure on the SOC and taking the focus away from their main responsibility of ensuring the company is secure. As noted in a blog by Komand [4] 'many SOCs take the term "operations" too literally and SOC personnel end up being technicians, making firewall changes and implementing security products instead'.

Additionally one thing that should be considered, particularly for internal SOCs, is an adequate separation of duties if additional tasks are being allocated to protect against the insider threat. If a malicious insider works as an analyst and, therefore, has data on how to best attack a company through vulnerability assessments, alongside having in depth knowledge of how the monitoring solution works, it will mean they have a much greater chance of successfully compromising the company.

According to Hewlett Packard [11] 'a mature SOC that is fully staffed, operationally mature and properly aligned to its mission and vision statements, with dedicated engineering resources, should be expected to absorb "spikes" in detections and return to a normal state over a short time'. However, if analyst time is filled with additional duties there may not be the bandwidth to achieve this.

In addition, the same article states ‘administrative tasks levied on top of analytical tasks in a SOC degrade overall results. Organisations often gauge that there are not enough events detected in the SOC and assign other non-detective tasks to ensure full utilisation of SOC analysts. A more mature response is to discover why there is a lack of detection and implement a plan to improve the SOC’s detection capability’.

5.7 Compliance

A frequent reason for utilising SOC services is to be compliant with certain regulations and SOC generated reports can prove that certain benchmarks are being met.

This is a valid reason for employing the services of a SOC, however, compliance and security are two different entities and there is a risk that the two can be confused. This can result in the belief that because a company is compliant it is also secure, which may not be the case.

If a SOC is used for compliance reasons then security needs to be considered separately in order to ensure that both needs are met.

This is summarised very well in an article on the Information Systems Security website [24] ‘attacks are becoming more frequent and sophisticated, pushing existing security capabilities to the limit, and regulatory compliance issues place added burdens on systems and network administrators’.

This can result in the belief that because a company is compliant it is also secure, which may not be the case.

5.8 Protecting the SOC

As noted in the NCSC guidelines [8], ‘a secure SOC protects itself’. The SOC is where all data on ongoing incidents is held and as such it is a target. Attackers will want to conceal traces of their activity and they will need to compromise the SOC to do so. Care must be taken that all security and monitoring procedures apply to the SOC as well.

As well as the fact that the SOC holds valuable data, there is also reputational damage and customer confidence to consider. If the SOC is breached and the breach remains undetected, it may call into question the ability of the SOC to perform an adequate service for its customers.

5.9 Threat intelligence

Threat intelligence is defined as ‘details of the adversary’s tools tactics and procedures’ [6] and the associated knowledge and data feeds to gain such information.

Outside of hunting activities, a SOC can only detect what it knows about, so threat intelligence plays a vital role in increasing the size of knowledge stores. There are many different sources of threat intelligence which can be generated internally by maintaining a database of known indicators of compromise from previous incidents. It can be gained from the security community at large and may be open source or a paid service, or it can be shared across organisations. There are many benefits to sharing threat intelligence across organisations as noted on the National Cyber Security Centre website [8]. However, care must be taken to protect confidential information.

6. Benchmarking

This section aims to provide suggestions for how to benchmark a SOC and areas that provide measurable criteria that can be assessed and compared to show where a SOC is improving. It will also highlight any weaknesses that need to be addressed.

6.1 Existing maturity models

As noted in section three, there are a number of existing maturity models that can be used to assess the maturity of a SOC. The most common of these is a combination of ITIL and COBIT, however, a holistic framework for classifying and rating a SOC is described in a Rhodes University paper on Classification of Security Operation Centres [25].

Applying a framework or maturity model to a SOC will give a good overview of current positioning, strengths and weaknesses and areas for improvement which can be tracked over time.

6.2 Identifying customer requirements, key contacts & assets

All SOCs, whether internal or external, will have customers. In order to streamline the response when an attack takes place, it will help to identify who these are ahead of time, alongside the key contacts who need to be alerted when an attack happens or when action needs to be taken.

A method for defining customer requirements should be used, most commonly this will be through a workshop to define use cases. Once these requirements have been captured, this can then feedback into deciding who key contacts are if an event occurs that hits one of the use cases.

In addition, appropriate service level agreements should be agreed at this stage along with defining the organisations assets, what they are and what the highest priority for protection is. This can help the SOC assess the impact of a threat or whether it may be a false positive.

6.3 Physical environment

There is a heavy requirement for teamwork within a SOC and particularly for an internal SOC. They may be dealing with sensitive information that the rest of the company should not have access to. With this in mind, it is vital to consider the physical environment for the SOC. Ideally, this will be a segregated area specifically designed for the SOC, but if this is not possible, then analysts should at least be seated together and with the required technology in close proximity.

6.4 Staffing metrics & plan for expansion

Although the number of staff required will vary between SOCs, it is important to identify the roles that need to be filled and how many staff will be required. This should take into account how many tiers of analysts will be required, what shift pattern the SOC will work and how many people will be required to fill this safely. All while taking into account holidays, sick leave, training, exams or anything else that may require some slack to fill the gap.

A fully staffed SOC should also be able to surge to respond to unexpected activity, such as a nationwide malware breakout or mass attack, but this should be a short term event.

At this phase, consideration needs to be made for what the indicators are that the SOC needs to grow and a plan should be put in place for how this growth will take place.

6.5 Training & progression plan

Analysts are unlikely to want to continue working at tier one indefinitely and will, usually, want to move onto more skilled or specialist work. A training plan should be put in place so that an analyst understands their pathway while working for the company and future options that are open to them. Alongside this, identifying the type of skills required for each role and how these skills may be acquired gives confidence to the analyst that they are being invested in and ensures that the SOC has the correct level of expertise.

6.6 Identifying leadership & senior sponsors

Without appropriate leadership and senior level support the SOC will struggle to carry out its mission as it will lack the appropriate authority.

It is therefore important to identify who the leadership for the SOC is, both in terms of day-to-day management and who has the authority to make final decisions as well as who is sponsoring the SOC from a board level and can make decisions at a high level regarding budget and defining the SOC mission.

6.7 Processes & procedures

Well defined processes that are easily accessible help to ensure that the SOC responds to events in a consistent manner and reduces the reaction time in a major event or when a less common event occurs. Areas that require processes should be identified and include what happens when something is detected, opening a ticket and what needs to be included, when and how incidents need to be escalated, out of hours and on call procedures and what happens at shift hand over.

Once identified, the appropriate processes should be designed and documented and then placed somewhere accessible so anyone who needs them will be able to swiftly find the appropriate process.

6.8 KPIs

KPIs will be unique to each SOC but should be defined in order to give a quantifiable measure of how well a SOC is doing, as well as areas for growth and improvement. These may tie into an existing maturity model or can be stand alone.

One metric that it can be particularly effective to measure is the detection rate and time to respond. Once a threat has been detected it calculates how long that threat was active before it was detected and how long before the threat was removed.

One metric states that effective security measures are those where protections last longer than the time to detect a threat plus the time to remediate that threat, i.e. MTP > MTD + MTR, MTP (Mean Time to Protect); MTD (Mean Time to Detect); MTR (Mean Time to Repair)' [9]. This can be used to assess how much protection needs to be given to a key asset.

Other KPIs will vary depending on individual goals and focus. However, a few potentials measures may include: [26] and [27]

- Staff retention rate.
- Operation audit result.
- Vendor SLA compliance.
- Ticket resolution rate.
- System availability and accessibility.
- Volume of events, incidents and tickets that were handled (both the number and the type).
- Resolution times.
- Number of employees.
- Headcount to ticket ratio.
- Number of employee certifications.
- Events/incidents generated per region, device, signature.

6.9 Identifying technology required & why

Although technology is vital to a successful SOC, it can also be used to mask a problem or can be ill-scoped. Therefore, it is important to identify the technological needs of the SOC and identify which piece of technology serves it best.

Furthermore, each purchase should be assessed over what it provides that is not already catered for and whether this is actually a requirement that will help the overall goal of securing the customer and ensuring business continuity.

It should be established that the SOC has the right technology to enable its mission and there are no gaps, but equally that each piece of equipment serves a purpose.

7. Testing the SOC

It is useful to devise ways of assessing a SOC in a measurable and repeatable way. This can be through automated or human tests and may or may not be done with the SOCs knowledge.

Either way this will aid in detecting gaps in the SOCs capabilities and where improvements can be made, but equally show what is being done well and the benefit people and assets are providing.

8. Crossover, compliance & additional responsibilities

As noted in section five, SOC staff are often tasked with additional responsibilities. The SOC may be responsible for compliance as well as security and the SOC may also be merged with a NOC.

While these are all valid ways of working, they do put a drain on resources and may mean a SOC is not able to respond as efficiently to incidents or its primary purpose.

Due to this, care must be taken to identify where these extra tasks are occurring and assess whether the SOC is the correct place for that work to take place. Where these tasks remain the responsibility of the SOC, it must be understood what impact this could have, what it may mean in the case of a major incident and if these tasks can be dropped in favor of a surge should the need arise.

9. Extra services

Extra services can be a valuable addition to a SOC, helping with staff retention and attracting industry specialists. However, they should only be considered when the basic SOC functionality is solid and operating at a satisfactory level.

When it is appropriate to add these extra services they need to be identified and then appropriate processes and procedures should be established, alongside what is expected from these roles.

This may include, malware analysis, incident response, forensic capability, hunting, SIEM engineers, threat intelligence and many others.

10. Growth plan

As the threat landscape is ever changing, the SOC will need to be in a continual state of growth otherwise it may stagnate and its ability to detect threats may decrease.

It will be necessary to prepare a growth plan for the SOC, preferably alongside the board level sponsor in order to plan for and be in a position to support this change. This should establish the intended growth in the short, medium and long term as well as how the SOC is expected to be performing and what success looks like.

11. Protecting the SOC

As the SOC is a valuable asset and key target, it will be necessary to put a sufficient amount of effort into protecting it. A plan should be established for how key assets will be secured, if the SOC will be monitored for signs of attack (and whether the SOC will do this themselves) and how a level of compliance will be proven. This may include external penetration tests and continual assessment of where vulnerabilities may arise.

12. Conclusion

In modern times, securing an organisation means protecting infrastructure, but also detecting when someone is attacking and being able to respond appropriately. As described throughout this paper, these are some of the services a SOC can provide.

Implementing a SOC is not simple, as SANS Institute describe it in their whitepaper on achieving a world class SOC ‘achieving the goal of better security depends on how that budget is allocated; what people, procedures and infrastructure are put into place; and how the security program is managed and optimised over the long term’ [10].

On a daily basis ‘most SOC teams are fighting fires with never enough staff, never enough time and never enough visibility or certainty about what’s going on’ [6], but with careful planning and effort put into ensuring the right people, processes and technologies are in place, along with a few other considerations a mature and effective SOC can be established.

13. Acknowledgements

Special thanks to Michael Parker and Josh Clark of the NCC Group SOC team for their assistance in writing this paper and for taking the time to provide details and a tour of the NCC Group SOC.

14. References & further reading

[1] http://www.ey.com/Publication/vwLUAssets/EY_-_Security_Operations_Centers_against_cybercrime/$FILE/EY-SOC-Oct-2013.pdf

[2] https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware

[3] https://www.computer.org/csdl/proceedings/hicss/2015/7367/00/7367c253.pdf

[4] https://blog.komand.com/4-experts-explain-the-best-strategies-for-a-successful-security-operations-center

[5] http://www.networkworld.com/article/2357938/network-security/137531-Managed-Security-Inside-a-working-Security-Operations-Center.html)

[6] https://www.alienvault.com/resource-center/ebook/building-a-soc/soc-team

[7] https://digitalguardian.com/blog/what-security-operations-center-soc

[8] https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide

[9] https://www.cybrary.it/0p3n/best-practices-for-security-operations-center/

[10] https://uk.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907

[11] https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA6-8216ENN.pdf

[12] https://blog.komand.com/defining-the-roles-responsibilities-of-your-security-team

[13] https://www.infosecurity-magazine.com/opinions/best-practices-for-the-soc-team/

[14] http://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html

[15] https://www.mcafee.com/br/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf

[16] https://www.rsaconference.com/writable/presentations/file_upload/tech-203.pdf

[17] http://www.csirt.org/publications/

[18] https://www.nist.gov/publications/computer-security-incident-handling-guide

[19] http://resources.infosecinstitute.com/security-operations-center/#gref

[20] https://www.nccgroup.trust/uk/our-services/cyber-security/products-and-cloud-services/socalive/

[21] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/may/socalive-introducing-a-safe-repeatable-and-scalable-way-to-

assess-security-operations-centre-soc-efficacy/

[22] https://www.nccgroup.trust/uk/our-services/cyber-security/penetration-testing-and-security-assessments/cyber-attack-readiness/

[23] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/march/we-see-the-world-in-black-blue-and-red-with-a-little-purple/

[24] http://ai2-s2-pdfs.s3.amazonaws.com/f5c6/8f1c3135ace2a71e31070e73453c4f3a190b.pdf

[25] http://icsa.cs.up.ac.za/issa/2013/Proceedings/Full/58/58_Paper.pdf

[26] http://www.securityinfowatch.com/article/10840065/metrics-for-success-security-operations-control-center-metrics

[27] https://countuponsecurity.com/tag/security-operations-center-key-performance-indicators/