What is a Security Operations Centre?

Introduction

A Security Operations Centre (SOC) is a team created to protect organisations from cybersecurity breaches by identifying, analysing and responding to threats. SOC teams comprise management, security analysts, and security engineers. A SOC liaises closely with an organisation's business and IT operations teams.

Of course, it's vital to communicate to all staff within any organisation that security is everyone's responsibility; a SOC is simply the central point for management of security issues.

According to an IBM-commissioned report, **Cost of a Data Breach 2021**, the average cost of a data breach among those surveyed is US$4.24m, reflecting a 10% increase in reported average cost, year-on-year. The report also revealed the average time for respondents to identify and contain a breach is 287 days.

Clearly, there is work to be done in better securing organisational data — and that's where the emerging and evolving concept of a Security Operations Centre (SOC) comes in.

To keep ahead of threats and monitor and respond to them, there's a growing need for a joined-up response, comprising security professionals, good technology and appropriate processes and procedures.

But before we get into the critical functions of a Security Operations Centre, (SOC) it's crucial to outline the broad functions of a SOC.

There is a myriad of descriptions of what comprises a SOC. This paper is an attempt to define what the critical functions of a SOC are, to help better understand what a Security Operations Centre does, and how it fits into the wider organisation and society.

Building blocks

A Security Operations Centre is a centralised business unit that deals with security issues at both the organisational and technical level. It comprises three building blocks: people, processes, and technology, for managing and enhancing an organisation's security posture.

Governance and compliance provide a framework, tying together these building blocks.

SOC staff monitors an organisation's information systems using telemetry from various sensors throughout the infrastructure.

A SOC is responsible for an organisation's overarching cybersecurity, which can include prevention and incident response (IR). By its very nature, a SOC forms a crucial part of an organisation's compliance and risk management strategy.

Security Operations Centres tend to have a much broader scope of responsibility than the more specialised CIRTs (Cyber Incident Response Teams). Many companies only have a SOC team, but no CIRT. It is also common for IR specialists to fall under the SOC umbrella rather than as part of a dedicated CIRT.

SOCs can be internal, external (managed), virtual or hybrid, involving a combination of in-house engineers and an external Managed Security Service Provider (MSSP), more of which later.

A SOC's primary functions include:

- To understand the physical and digital assets, systems, risks and vulnerabilities of the organisation's environment
- Monitoring the security of business assets, including the network, users, and systems
- Data collection and correlation
- Threat detection, including identifying anomalies, threat hunting capabilities, and the use of behavioural analysis tools and techniques
- Alert triage to analyse and prioritise alerts
- Incident analysis, assessing the severity of the threat, and the impact it may have on the organisation to formulate an appropriate response
- Incident review to gather information about attack patterns and techniques, to assess the need for more monitoring rules

Vulnerability management and firewall management may not be considered primary functions of a SOC, but they are often incorporated.

People, Technology, Process

If we agree that a SOC comprises people, technology and process, it's worth taking a moment to better understand what's meant by this.

In terms of **People** — this means the human resources that are required within a SOC to understand the output and context of information received via use of technology. Your people — talent — need to hold a deep understanding of the risk posed to the business.

The people involved in a SOC must be predominantly experienced security professionals with the ability to understand, triage (prioritise) and investigate security incidents from a selection of appropriate tools including. Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Security Orchestration, Automation and Response (SOAR) for example.

A contemporary SOC team must be capable of progressively and continuously adding detection capabilities within the tools used and map them against known frameworks, such as **MITRE ATT&CK.**

From a **Technology** perspective, we mean the tools. that receive and allow analysis of logs or data from source systems to ascertain if a potential security incident is occurring. Typically, this is known as a Security Incident and Event Management (SIEM) platform.

It also includes the technology required to glean (threat) intelligence, either through tools or collected and enriched separately. In more mature environments, there may also be technology in place, in terms of tools, or the ability to action a response to respond to alerts and provide some form of containment (as a minimum).

Finally, **Process** revolves around creating a set of plans or processes that tie together the technology and capabilities of a SOC. These plans should incorporate the business objectives and strategy.

By consolidating security experts and relevant data into a central location — the SOC — threats are quickly identified and dealt with more efficiently and effectively. A SOC leverages people, processes, and technology to reduce cyber security risks, via improving organisational security, information and communication.

The purpose of a SOC and why you need one

> "A security operations centre (SOC) can be defined both as a team, often operating in shifts around the clock, and a facility dedicated and organised to prevent, detect, assess and respond to cybersecurity threats and incidents, and to fulfil and assess regulatory compliance."
>
> **Gartner**

Having briefly outlined what a SOC is, we should now consider its purpose.

For small organisations, it may not make (financial) sense to create a dedicated internal SOC team. But as organisations grow, so do the risks and cost of cyberthreats. Failing to prepare, organise and arm a team of qualified security operations professionals can become an expensive mistake.

This is especially true among organisations that deal with sensitive information, such as financial information, health records or trade secrets.

Today, a majority of organisations need a formal organisational structure — a SOC — that holds responsibility for threat detection and response or Active Defence. A SOC forms the operational side of cybersecurity threat management.

There needs to be an efficient process for detection, mitigation and prevention of threats in place.

SOC teams hold dual core responsibilities:

1. Maintaining security monitoring tools

A SOC should maintain and update tools regularly and be aware that monitoring rules continually evolve with the threat landscape. It's crucial that tools and technology are managed, as without them, a SOC cannot hope to adequately secure organisational systems and infrastructure.

2. Investigation of suspicious activities

The purpose of your 24/7/365 SOC team is to investigate suspicious and / or malicious activity within the organisation's networks and systems. SIEM software or analytics software will issue alerts which the SOC team must then analyse, triage and ascertain the extent of the threat.

A SOC helps safeguard a business from cyberattacks, preventing disruption that may relate to, or be caused by, cyberattacks and works towards continuous improvement of cyber security resilience.

Active, continuous monitoring for security threats and appropriate responses to those threats is a key function of any SOC.

Security events must be collated, and appropriate notification efficiently disseminated to relevant stakeholders. A SOC needs the relevant resources to interpret, validate and respond to threats, to neutralise them.

Intelligence must be gleaned from multiple sources, then enriched or validated (via automated and / or human means) to gain better contextual awareness or reduce the threat level to the organisation.

Creating a SOC means a higher level of incident response, thanks to around the clock operations, coupled with developing greater threat intelligence and rapid analysis.

When to create a SOC

You may have some form of operational security now, but there are many reasons to re-evaluate the effectiveness and capabilities of what it provides the organisation,

including:

- The organisation is handling more sensitive data
- The threat landscape has changed, or become more concerning, and requires improved security
- The organisation (or attack surface) has grown larger — and bear in mind the security issues surrounding remote working
- Your current managed security service provider (MSSP) doesn't deliver the capabilities needed by the business

Reducing complexity

Although developing and creating a SOC can represent a major cost, in the long run, such a facility prevents the cost of reactive, ad hoc security measures, and, of course, protects from the financial damage caused by breaches.

Having a SOC embedded in your organisation will also naturally reduce the complexity of investigations, as SOC teams can streamline their investigative efforts, by coordinating data and information from a variety of sources. With full visibility into the network environment, for example, SOC teams can simplify drilling down into logs and forensic information.

Up to September 2021, there were 1,291 data breaches — compared to 1,108 breaches in 2020.
Security Magazine

A **2019 Ponemon / IBM report** suggested it takes the average US company an enormous 206 days to detect a breach — plus another 73 days on average to remedy the breach. We already know this figure, according to another **IBM report** in 2021, has risen to a higher total of 287 days.

And the costs run into millions of dollars. A breach lifecycle of more than 200 days is 37% more expensive than a breach lifecycle of less than 200 days (US$4.56 million vs $3.34 million).

Further, the 2019 report reveals:

- Security automation technologies could potentially half the financial impact of a breach
- Extensive use of encryption can reduce total cost of a breach by US$360,000
- Data breaches cost companies around US$150 per lost or stolen record
- Breaches originating from third-parties cost organisations US$370,000 more than average
- Companies with less than 500 employees suffered average losses of more than US$2.5 million

Around two thirds (67%) of the financial impact of breaches are felt within the first 12 months, 22% in the next year and 11% in the third year after the incident. Long-tail costs are more acute in highly regulated industries such as financial services, healthcare and energy.

At present, not every organisation has a SOC, or understands the requirement for one. A CREST internal survey revealed increasing boardroom buy-in to the concept, but there is a gap in understanding and funding for a fully functioning SOC.

While there are myriad reasons why a SOC might be required, some examples include:

- Maintaining the confidentiality and integrity of sensitive data — accessible by staff on the premises, by remote staff, or by customers and partners
- When running an online service for the public
- In organisations with dispersed offices, where a unified security function delivers cost savings
- In situations where large amounts of (sensitive) data needs to be shared with other organisations (such as finance, health and government)
- Where a single point of visibility over all threats is required

Core processes a SOC should deliver include:

Alert triage — Collecting and correlating log data, the SOC provides tools that allow analysts to review that log data and detect security issues.

Alert prioritisation — SOC analysts use their knowledge of the organisation, the wider business environment and the threat landscape to prioritise alerts and rapidly ascertain which events represent real security incidents.

Containment — On discovering an incident, SOC staff is responsible for threat mitigation and escalating it for remediation and recovery.

Reporting — Documenting the organisation's response to an incident.

In developing a SOC, there needs to be preliminary work around understanding organisational needs, the landscape in which it operates and any weak points from a cyber security perspective.

A SOC cannot function in isolation, although it functions as the operational part of organisational security; typically separate from policy defining and audit / compliance and governance elements.

There are several issues which need to be defined, including:

- A strategy and objectives
- Inventory, budget and resources allocation
- Capabilities
- Timeframe, and
- Technology required.

Only then may a SOC be formed that is closely aligned to the business, rather than following generic guidelines or mirroring other existing SOCs.

What a SOC does

A SOC's primary function is security monitoring. This task involves centralised collection and correlation of log data from all elements of the infrastructure, applications and endpoints, which is then used to identify any deviations from the 'norm'.

This log data can be collected from cloud infrastructure, intrusion detection systems, firewalls, web applications, active directory servers, anti-virus software and industrial control systems, for example.

The SOC needs to monitor any system which can provide insight into the security or status of the organisation's network and systems connected to it.

There are no clear benchmarks or frameworks to base the organisation or function of a SOC on.

However, in 2019, Gartner launched its Continuous Adaptive Risk and Trust Assessment (CARTA) framework, developed from the realisation that a black and white way to monitor threats was simply not enough.

Gartner sees CARTA as a strategic approach for organisations to manage evolving digital world risks by deploying security that moves at the speed of digital business. It suggests the SOC must move away from an 'allow / deny' gating model towards a far more dynamic, context-aware and adaptive structure.

While CARTA can be a useful starting point in any approach to organisational information security, when ascertaining which type of information to collect, which systems to collect information from and which correlation method to use, the most important aspect is to focus on information relevant to your organisation — rather than on what is considered customary to collect.

Critical functions of a SOC can ultimately be boiled down to a brief list:

Awareness of all IT assets — hardware, software and information or data. Your SOC should have a full, detailed picture of every element running on your infrastructure, including its owner and criticality, to assist in understanding developing threats to them. Assets must include everything, from cloud services to physical infrastructure.

Log management. Traffic, incidents and anything of interest must be continuously monitored and logged, so the organisation and any authorities can complete forensics if an incident or breach occurs.

Proactive detection of malicious network and system activity. Probably the most critical function of a SOC. Organisations need to know as quickly as possible if there is a breach — or chance of a breach — and what urgent action to take. You don't want to wait the average 206 days it takes US companies to detect a breach.

Vulnerability management. Again, constant work to assess any potential gaps in your network allows for the holistic oversight in terms of organisational vulnerabilities, and which areas might be most vulnerable to existing and emerging threats before you get hit with them.

Threat awareness. Simply put, maintaining keen, constant awareness of the ever-evolving threat landscape allows your SOC to tweak defences — both physical and virtual — before any threat hits the organisation.

SOCs can be involved in most of the incident management process. This might include:

- Integration, management and review of traffic feeds
- Protective monitoring
- Initial triage and analysis
- Alerting and response
- Incident management
- Root cause analysis
- Correlation management.

But before creating a SOC, there must be agreement across the organisation on what constitutes an EVENT and what constitutes an INCIDENT. This is obviously of crucial importance for the security analysts.

Events

An event can be described as any activity that is deemed as important to monitor. individual events may not be considered unusual and may just be day-to-day activity needed to identify anomalies, whilst others may be indicators of an issue, for example virus detection. Events might include:

- Server logs, including Log-on activity
- Firewall traffic logs
- Proxy logs
- Anti-virus or EDR logs

Incidents

Meanwhile, an incident is seen as something that is potentially or actually a threat or a violation of information security policies or standards. **NIST** describes incidents as: "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."

Incidents might include:

- Unauthorised use of system privileges
- Denial of Service attacks on a web server
- Sending malicious files to a targeted user
- Stealing sensitive information and blackmailing the owners

As soon as a security incident is confirmed, a SOC acts as 'first responder'. SOC analyst staff will perform tasks such as shutting down or isolating endpoints, terminating any harmful processes (or preventing them from executing) and deleting files, for example.

The overarching aim should always be to respond to the correct, required extent deemed necessary, while ensuring minimal impact on business continuity.

Incident management process flow

Log the incident

First steps must always be to inform relevant parties of the identified incident, via appropriate pre-agreed channels. A SOC team member from the incident handling team should be charged with responsibility for capturing all necessary details and data related to the incident and reporting it.

Classification

Classifying incidents under pre-agreed and understood categories will speed up the incident handling process and save time for deeper investigation.

Prioritise incident

Assigning proper priority to an incident ticket ensures the incident is addressed in a timely fashion.

Investigate and diagnose

When an incident occurs, the incident response team should perform a deep analysis of the incident and create a report.

Incident closure

The primary goal of incident management is to resolve it swiftly and efficiently. Closing the ticket after effective communication to concerned parties is a crucial step in the incident handling process.

Remit of the SOC

While each SOC management team should decide on the exact functions required, the decision as to the remit of any SOC includes, but is not limited to:

- Budget
- Whether a third-party supplier is used
- Willingness to share information feeds with a commercial supplier
- Internal willingness and / or capability to perform forensic investigations
- How business continuity is managed
- Whether the SOC is internal or external (or hybrid)
- Existing understanding of the range of threats
- How bespoke the SOC functions need to be — a generic set up will be less costly

While detecting and responding to (cyber) threats and keeping data held on corporate systems and networks secure are primary functions of any SOC, there are broader functions, too.

These include increasing (network and organisational) resilience by perennial study of the changing threat landscape (both malicious and non-malicious, internal and external). There is also a need for a level of expertise within the SOC team that is sophisticated enough to identify and address negligent or criminal behaviours.

Finally, creating a bank of business intelligence regarding user behaviours to help shape and prioritise technology development is a crucial element of a contemporary SOC.

SOCs are often built with several functions — commonly thought of as a hub-and-spoke architecture. Around the central SOC hub, the 'spokes' could include vulnerability assessment solutions, governance, intrusion prevention systems (IPS), user and entity behaviour analytics (UEBA), endpoint detection and remediation (EDR), risk and compliance (GRC) systems, application and database scanners, and threat intelligence platforms (TIP).

Size of a SOC

The exact size of your SOC depends on the nature and size of your business. Organisations with more critical sensitive data, such as those in healthcare or financial services, should consider larger teams, and more hardware and software investment.

In a paper, the Dutch **National Cyber Security Centre** advises starting small. A small SOC can then grow and evolve with the organisation; while ensuring "the planning, roadmap and implementation of a future SOC are realistic."

It goes on to suggest that: "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."

Scope

While a **Security Information and Event Management (SIEM)** system — software designed to interpret log data from several sources and correlate it with cyberattacks and other security incidents on the organisation's network — is widely considered a core tool in the SOC's arsenal, essential for data analytics and correlation, in many cases, a Security Orchestration, Automation and Response (SOAR) platform — to integrate alert sources with Threat Intelligence — is considered sufficient, or perhaps even just a Managed Detection and Response (MDR) approach.

Threat intelligence (TI) is also key. Threat intelligence is usually defined as information from external sources regarding vulnerabilities and cyber threats. The information is used to assess events relating to systems and within the network.

Key SOC functions

Understanding available resources

A SOC holds responsibility for two asset types — the devices, processes and applications it is charged with safeguarding; and defensive tools at its disposal to ensure proper protection.

The SOC can't safeguard devices and data it cannot 'see.' Visibility and control must be enabled, from devices to the cloud, otherwise there may well be 'blind spots' in organisational network security.

A SOC must have a holistic view of the organisational threat landscape, and not only of the endpoints, servers and software used, but also any third-party services and traffic flowing between assets.

A SOC must keep detailed records and maintain full understanding of the cybersecurity currently enabled, along with all the workflows used in the SOC, to increase agility and ensure peak efficiency.

1. Preparation and preventative maintenance

Even well-planned, equipped and agile response processes are no match in preventing problems from occurring. To help keep attackers at bay, the SOC must implement preventative measures, which can be divided into two main categories, as follows:

Preparation

Analysts and staff must keep well informed on the newest security innovations, cybercrime issues and trends, and any new threats on the horizon. This vigilance can help inform creation a security roadmap — to deliver direction in ongoing cybersecurity efforts. It can also help formulate a disaster recovery plan — written guidance for worst-case scenarios.

Preventative maintenance

This could include action taken to make successful attacks harder to achieve, which may involve regularly maintaining and updating existing systems; updating firewall policies; patching vulnerabilities and whitelisting, blacklisting and securing applications. However, many of these actions are down to normal infrastructure team activity, and the SOC role merely provides guidance on preventative maintenance and remediation management for vulnerabilities.

2. Continuous proactive monitoring

The SOC's toolkit should be capable of scanning the infrastructure — such as the network, cloud and endpoints — 24/7/365, and able to flag any inconsistencies or suspicious activity.

Around-the-clock monitoring allows the SOC team to receive immediate notification of emerging threats, which in turn provides the best possible chance of preventing, or at least mitigating harm.

SOC tools may include:

Security Information and Event Management (SIEM) software. A SIEM solution gathers and analyses activity from different resources across the organisation's IT infrastructure.

Endpoint Detection and Response (EDR) is another software solution which can detect threats and respond to them. It can analyse the threat and provide analysts with salient information, such as where it emanated from, how it started, which parts of the network it has affected and how to stop it.

Security Orchestration Automation and Response (SOAR) software helps the SOC team — especially smaller teams — improve efficiency by better managing threats and vulnerabilities, automating repetitive tasks and responding to security incidents. An example of this might be automatically deleting phishing emails from employee's inboxes.

eXtended Detection and Response (XDR) software collects and automatically correlates data across multiple security layers, such as email, endpoint, server, cloud workload, and network. The most advanced XDR solutions employ behavioural analysis to teach systems the difference between regular day-to-day operations and actual threat behaviour, minimizing the amount of triage and human analysis required.

3. Log management

A SOC holds responsibility for collecting, maintaining, and reviewing the log of all network activity and communications for the entire organisation. This data helps define a baseline for "normal" network activity. It can expose the existence of threats and be used for post-incident remediation and forensics.

4. Alert ranking and management

SOC staff must be ready to examine alerts, discard false positives and determine the size and scope of any actual threats and what they're targeting. This allows for appropriate triage, and the ability to handle the most urgent issues as a priority.

5. Threat response

Upon confirmation of an incident, the SOC must function as first responder, shutting down or isolating endpoints, terminating harmful processes (or preventing them from executing) and deleting files, for example. The goal is to respond to the extent necessary while having as small an impact on business continuity as possible.

6. Root cause investigation

A SOC holds responsibility for ascertaining exactly what happened when, how and why in the event of a cyber security incident. Post-attack / incident investigations should involve using log data and other information to help trace the problem to its source, to help prevent similar issues from occurring in future.

7. Security refinement and improvement

Cybercriminals constantly refine tools and tactics. To keep ahead of them, your SOC team needs to continuously implement improvements. Improvements can include 'live' practices such as red-teaming (subjecting the organisation's plans, programmes, ideas and assumptions to adversarial analysis and challenge), blue teaming (keeping the organization safe from attackers by understanding their tactics, techniques and procedures (TTPs) and evolving company's defences) and purple-teaming, which ensures proper information sharing between Red and Blue teams, maximizing their respective and combined effectiveness.

8. Compliance management

Several SOC processes are guided by established best practices. Others are governed by compliance requirements. Regular audits of a SOC's systems is necessary to ensure compliance with regulations, which may emanate from the organization, the industry, or governing bodies.

Examples include GDPR, (General Data Protection Regulation) HIPAA, (the Heath Insurance Portability and Accountability Act) and the PCI DSS (Payment Card Industry Data Security Standard).

Working within the remit of such regulations helps safeguard the organisation's sensitive data. Regulatory compliance can also shield the organisation from reputational damage and any legal challenges resulting from an attack.

In short, a SOC monitors, assesses and appropriately reacts to any threats made towards the organisation. Its most critical function is to protect an organisation from threat.

Virtual, managed and hybrid SOCs

It wasn't very long ago that a SOC was considered something only the largest enterprises should enable. But nowadays, smaller organisations are developing 'lightweight' SOCs, especially as the threat landscape evolves and attacks become ever more prevalent.

There are myriad ways to choose how to set up and run an effective Security Operations Centre.

These include the hybrid SOC, a team which brings part-time, in-house staff together with outsourced experts. Another growing option is a virtual SOC, with no physical facilities, but can comprise a team of in-house staff which also work in other roles, or a remote team.

A managed SOC brings all the benefits of a professional cyber security team to your organisation, without the associated full-time costs, and provides a higher level of experience and expertise than might be immediately available to an internal SOC.

Most SOCs operate on a 'tiered' basis:

Tier 1 involves monitoring, opening alerts and closing false positives. Staff working at Tier 1 are alert analysts.

Tier 2 involves deeper investigations, mitigation and recommendations. At this level, staff are incident responders.

Tier 3 involves advanced investigations, prevention, threat hunting, forensics and counterintelligence. While Tier 1 and Tier 2 can be handled by regular security analysts, Tier 3 requires expert analysts.

The SOC manager sits above all three tiers.

Below Tier 1 operations, automated investigation and remediation, as a response to well-known attacks, can take place. Tier 1 responses will deliver high speed remediation. Tier 2 responses bring deeper analysis and remediation, while at Tier 3, we see proactive hunting and advanced forensics.

This tiering is helpful in considering whether to create a **hybrid SOC** model in your organisation.

For example, some companies choose to outsource Tier 1 and 2, 24/7/365, while maintaining Tier 3 level specialists inhouse.

Virtual SOCs (VSOCS)

A virtual SOC (VSOC) has no physical presence, no dedicated facility, nor dedicated infrastructure. A VSOC is a web-based portal built on decentralised security technologies, which allows remote teams to monitor events and respond to threats.

An increasingly popular concept, the VSOC is considered to be a cost-saving SOC, in that the sometimes-significant costs of onsite hardware and other important infrastructure are avoided.

Researching, choosing and purchasing an inhouse infrastructure for a SOC can be not only daunting, but expensive. Jumping into a VSOC environment negates organisational concerns over time, effort and cost of setting up inhouse.

The VSOC team, of course, can be relied on to respond swiftly and reliably in the event of an incident. The expertise already offered via a VSOC's staff is another issue solved. Creating a SOC inhouse comes with staffing and talent cost headaches.

However, VSOCs can seem to deliver a reactive approach. With decentralised technologies and processes, there may well be security gaps — making threat detection and response less efficient.

Consider the challenges of data sovereignty and security when thinking about VSOCs. You must ascertain whether your data includes anything that has residence requirements. Where, then, will it be stored within a VSOC arrangement?

Check whether your proposed VSOC operation is 24/7/365. And remember that using part-time, remote staff can leave gaps in your SOC provision.

Of course, a VSOC can be bolstered using automation, SIEM technology and good analytics.

Outsourcing a VSOC might increase the SOC's security capabilities and bring greater access to expert resources, but it will reduce internal visibility across the environment. Be mindful that an outsourced SOC may lead to slower response times if an event escalates.

And be mindful that VSOC services can act as an adjunct to your own in-house SOC provision. You might wish to combine both, and as the need for SOC services grows, expand your inhouse team.

Managed SOCs

A **Managed SOC** is one which is outsourced and managed by a **trusted external provider.** This means lower costs, access to experienced professionals, and fast response times.

Outsourcing your security operations can also mean access to superior technology. Your overstretched IT department will be grateful that your Managed SOC has all the latest hardware and software — the lifeblood of their business, after all.

Being wholly responsible for managing threats for a number of organisations means the Managed SOC provider can ill afford to fall behind in terms of equipment, knowledge and expertise.

A Managed SOC will also ensure proper data storage and protection, if required. But, as with the VSOC, the issues surrounding data sovereignty and security must be taken into consideration. Does your data include anything that has residence requirements? Where, then, will it be stored within a Managed SOC?

And who owns the technology used within the Managed SOC at the end of the contract / relationship?

Choosing the right level and style of Managed SOC is crucial, and it's worth taking the time to do your due diligence. Look for recognised, reputable industry players, which offer high levels of customer service, certified technicians, and around-the-clock support.

Hybrid SOCs

As you've probably already ascertained, there are several ways of setting up a SOC, to best suit your needs, budget and level of expected threats. A hybrid SOC is a way of combining different types of SOC provision, as mentioned above.

Outsourcing IT services is hardly a new concept, but it's worth remembering why we do it — mainly for flexibility, rapid scalability and cost effectiveness.

For example, you might have a small SOC team in-house, working 9-5, but employ a VSOC or Managed SOC provider outside of normal office hours.

You might decide the best model for your organisation is to completely outsource SOC provision, mindful of the tools, expertise and experience you can access from day one.

Hybrid model avoids some of the pitfalls of keeping provision in-house — and of outsourcing SOC services completely. Be mindful that in-house staff can become resentful of external service providers; feeling like their jobs may be under threat. Senior IT staff or your in-house CISO or SOC Manager must ensure good relations between internal and external staff.

It's also vital to ensure the external service provider (often known as a Managed Security Services Provider, MSSP) is familiar with your organisational culture, operations and functions. There must be a clear contract drawn up to define roles and responsibilities, and to help avoid gaps in security service provision.

Whichever model you choose, communication is perhaps as vital as technology and staff.

SOCs vs CIRT (cyber incident response team)

Years ago, it fell on the IT department to handle security issues. As the threat of cyber attack grew, so did the concept of a SOC, set up to handle organisational cyber security. And with the growth in SOC provision, there arose the concept of the CIRT.

A SOC is the broad, first line of defence, but if and when any threat is identified, this can be escalated to a Cyber Incident Response Team, or CIRT. These teams are sometimes also referred to as a CSIRT, or Computer Security Incident Response Team. It could also be called a CERT (Computer Emergency Response Team).

A CIRT can often comprise senior members of the SOC and is described as a centralised function for information security incident management and response. A CIRT will include security experts holding responsibility for incident management, especially receiving, analysing and responding to security incidents. They can operate independently or come under the guidance of senior SOC staff.

Typically, a CIRT will include security incident response experts, security architects, analysts and engineers, security managers, department heads and C-level operators, including the CISO.

A CIRT's remit might include:

- Forensic investigation of attack causes, encompassing discovering the attack timeline and lessons learned
- Development of security strategies to assist the organisation's threat prevention
- Incident management — including creating an incident response plan, to ensure rapid, effective response
- Threat hunting, leveraging threat intelligence from the SOC to detect threats
- Root Cause Analysis (RCA) and remediation

Like a SOC, it might not be appropriate for an organisation to have an in-house CIRT team, but its generally considered good practice to keep IR specialists on a retainer, so they can be called upon swiftly in worst case attack scenarios.

While a SOC can hold responsibility for incident response, it's better to have a separate CIRT team or function on hand, keeping the SOC team free to continue monitoring and protecting while the current attack is dealt with by the CIRT team. Where there is an internal or external CIRT, the SOC team can — and should — assist the CIRT in gathering all the information needed to deliver an effective response to threats.

Roles within the CIRT should not only include IR expertise, but also legal, marketing and public relations experts — to manage and mitigate the 'fall out' from the attack.

The CIRT team, just like the SOC team, can evolve over time. It may initially meet on an informal, ad-hoc basis, but as the organisation, threat landscape and organisational infrastructure grow, it may develop into a full-time function, as needs dictate.

Who should you employ in the SOC?

Staffing

A SOC's functions are usually overseen by a **SOC manager**. Such a person should be capable of directing all SOC operations. They hold responsibility for ensuring a clear information flow between analysts and engineers. The SOC Manager is the one who hires; organises and / or delivers training; and creates and executes the agreed cybersecurity strategy. Of course, a SOC manager will also direct and orchestrate organisational response to security threats.

Security analysts are the first line of defence in the SOC, acting as cybersecurity first responders. They can be subdivided into tiers, as described in the table below.

SOC analysts are organized in four tiers. Firstly, Security Information and Event Management (SIEM) alerts go to Tier 1 analysts who are empowered to monitor, prioritise and investigate such alerts.

Real threats identified by T1 analysts are then passed to a Tier 2 analyst, who should generally hold greater security experience. The T2 analyst will conduct deeper analysis, followed by a containment strategy.

Critical breaches are escalated to the Tier 3 (senior) analyst level, who will then manage the incident. SOC Managers are considered to be Tier 4 analysts, responsible for recruitment, strategy and direct management of SOC staff when major security incidents occur.

The analysts' role, broadly speaking, is to report any cyberthreats, and implement changes required to continue protecting the organisation. They're considered the last line of defence against cybersecurity threats, work alongside security managers and cybersecurity engineers, and usually report to the CISO.

Security engineers — software or hardware specialists — are charged with maintaining and updating the SOC's tools and systems. They should be capable of providing documentation other team members require, such as digital security protocols.

Above these roles there will often sit a **CISO** — Chief Information Security Officer. This C-suite leadership position holds responsibility for establishing security-related strategies, policies and day-to-day operations. The CISO reports directly to the CIO or CEO, informing and reporting to the board in regard to security issues.

In larger organisations (like multinationals), there may also be a **Director of Incident Response (IR)**, with overall responsibility of managing incidents, and explaining security requirements to the organisation whenever there is a significant breach.

Role title	Required skills and qualifications (for example)	Day-to-day activities
Tier 1 Analyst Alert Investigator	Web programming (Python, Ruby, PHP); scripting languages; basic security certifications (CompTIA Security+) sys admin skills.	Configures and manages security monitoring tools. Prioritises and triages alerts and / or issues to determine whether real security incidents are occurring.
Tier 2 Analyst Incident Responder	Similar to Tier 1, but with greater experience, including IR. Should be capable of advanced forensics, malware assessment and threat intelligence. Ethical hacker certification or training is advantageous.	Receives incidents. Conducts deep analysis. Correlates with threat intelligence to identify the threat actor, nature of the attack, and systems or data affected. Defines and executes strategy for containment, remediation and recovery.
Tier 3 Analyst Subject Matter Expert / Threat Hunter	More experienced than a Tier 2 analyst, including high-level incidents. Should be acquainted with pen testing tools and cross-organisation data visualization. Malware reverse engineering, and capable of identifying and developing responses to new threats and attack patterns.	Conducts regular vulnerability assessments and pen tests. Reviews alerts, industry news, threat intelligence and security data. Hunts threats and seeks unknown vulnerabilities and security gaps. When a major incident occurs, teams with Tier 2 Analysts in response and containment.
Tier 4 SOC Manager Team Leader	Keen project management skills, incident response management training and strong communication skills.	Hiring and training. Oversees defensive and offensive strategies. Manages resources, priorities and projects. Direct team management when responding to business-critical security incidents. Organisation contact for security incidents, compliance, and all security-related issues.
Security Engineer Support and Infrastructure	Computer science, computer engineering or information assurance degree. Certifications such as CISSP.	Software and / or hardware specialist, ideally experienced in security aspects of information systems. Creates solutions and tools to help organisations deal with operational disruption of. Note: Sometimes security engineers are employed within the SOC, other times they simply support the SOC as part of development or operations teams.

Table — Roles within the SOC, Edited from **https://www.exabeam.com/security-operations-center/security-operations-center-roles-and-responsibilities**

Reporting and analysis

Measuring the effectiveness of the SOC

Organisations must measure SOC team performance to continuously improve their processes. Here are a few **important metrics** that serve to demonstrate the scale of activity in the SOC, and how effectively analysts are handling the workload.

Metric	Definition	What it Measures
Mean Time to Detection (MTTD)	Average time taken to detect incident	How effective the SOC is in processing important alerts and identifying real incidents
Mean Time to Respond (MTTR) or Closure / Escalation Time	Average time before SOC takes action to detect and escalate the threat	How effective the SOC is at gathering relevant data, coordinating a response, and taking action
Total cases per month	Number of security incidents detected and processed	How busy the security environment is and scale of action managed by the SOC
Types of cases	Number of incidents by type: web attack, attrition (brute force and destruction), email, loss or theft of equipment, etc.	The main types of activity managed by the SOC, and where preventative security measures should be focused
Analyst productivity	Number of units processed per analyst — alerts for Tier 1, incidents for Tier 2, threats discovered for Tier 3	How effective analysts are at covering maximum possible alerts and threats
Case escalation breakdown	Number of events that enter the SIEM, alerts reported, suspected incidents, confirmed incidents, escalated incidents	The effective capacity of the SOC at each level and the workload expected for different analyst groups

A SOC's effectiveness can perhaps best be measured by using the services of Red, and / or Purple Teams.

Other resources required to measure the effectiveness of the SOC include:

People

The SOC board needs to include staff with deep technical and business knowledge. They needn't be permanent members of the SOC and can undoubtedly operate as a virtual team. Keeping experts on hand that can serve as an extension to the SOC team during attacks will increase success.

While certifications might not be a valuable metric, you can still track how staff improves over time. Nurturing staff proficiency in a specific domain is a measurement you could use to demonstrate your SOC team's quality, maturity, and knowledge.

And, of course, internal or external training will bolster existing skill sets. **Technology**

We've already stressed how vital up to date technology is to the success of a SOC. If appropriate hardware and software lie beyond the budget, consider an outsourced SOC function. Remember, the success of your technology will be measured by how it adds value to the organisation.

Policies

Success can be measured against policies created to describe the roles, responsibilities and IR processes involved in the SOC. Such policies set expectations for all stakeholders, as well as the authority to act when attacks occur, and the consequences of not adhering to the policies.

Benchmarks can be set under each aspect of such policies.

Planning

The SOC needs a vision which aligns with organisational objectives, priorities and risk posture. Maintaining alignment with the organisation and keeping the SOC team and technology running requires careful budgeting and resources.

And be sure to calibrate expectations. If it happens that someone outside the SOC team finds a threat or intrusion, what should they do? Who should they report it to? Plan the steps required to engage with such a situation, and what questions to ask before escalating it.

Be sure to strike a balance between reporting and feedback on the SOC's success and not over-delivering information to interested parties within the organisation. By delivering every detail of every metric, you'll make it hard for others to ascertain what's most important.

Consider which metrics highlight the success of the SOC. For example, time to respond / resolve might not look good on paper, out of context.

Decide which metrics you'll deliver and in what format. A good start is to highlight the number of incidents and escalations that have occurred over the agreed reporting period, with a status field and incident category.

Include the incident remediation techniques used and be sure to provide enough context for a less technical reader to understand. This context will help build bridges between the SOC and the rest of the organisation, helping improve the overall organisation's security culture.

Warning

This Guide has been produced with care and to the best of our ability.
However, CREST accepts no responsibility for any problems or incidents arising from its use.

CREST

For further information contact CREST at:

www.crest-approved.org