— A journey of a thousand miles begins with a single step.

A Chinese proverb

— Without a measureless and perpetual uncertainty, the drama of human life would be destroyed.

Winston Churchill

1 Introduction

Protecting confidentiality and integrity of data, while ensuring availability of digital assets and key technology systems is crucial for operating any business in the bold new hyper-connected universe. An effective Security Operations Center (SOC) is a primary means and plays a key role to achieve this goal. As the newer technologies like machine learning, IoT, Blockchain, autonomous and connected vehicles and others are becoming crucial for business success, concept of a modern SOC is also going through an evolution process. A modern SOC must provide capability to effectively manage risk associated with traditional as well as emerging technologies.

This book is a brief guideline for information security leaders and practitioners to understand implication of different SOC options and how to build and operate a successful SOC that meets their business needs and achieves goal of protecting digital assets. The book starts with an introduction to SOC and then builds on basic concepts to achieve excellence in building and operating a modern SOC. The objective is to provide the reader a complete guide, starting from building business case, acquiring needed technologies, hiring and training people for SOC operations, and building a governance model for measuring success and for continuous improvement.

1.1 What is a Security Operations Center (SOC)?

A Security Operations Center (SOC) is typically an organization inside a business that is responsible for protecting critical business assets by continuously monitoring emerging threats, collect notable security events, analyzing and prioritizing these events, and responding to security incidents.

Typically a SOC consists of components as shown in Figure 1.1, with technology stack at the core, wrapped with people, processes, and a governance model:

- ***Technologies*** for collecting log and other types of telemetry data, storing data, and processing/analyzing data. Main technologies used in SOC include Security Information and Event Management (SIEM) tool, log collection, network sensing, ticket/incident management, forensic tools, and vulnerability management tools.

- ***People*** with different level of expertise in diverse areas including networking, operating systems, applications, operations management, scripting, Python, vulnerability management, incident handling, forensics and others.
- Defined ***processes*** for tasks under the scope of SOC. While there are many SOC processes, effective incident detection and incident management is a key process for success of every SOC. A SOC may also rely on other IT systems/processes like asset management, change management, patch management etc.
- SOC ***governance*** structure that enables SOC management and continuous improvement while ensuring the business objectives of SOC are achieved.

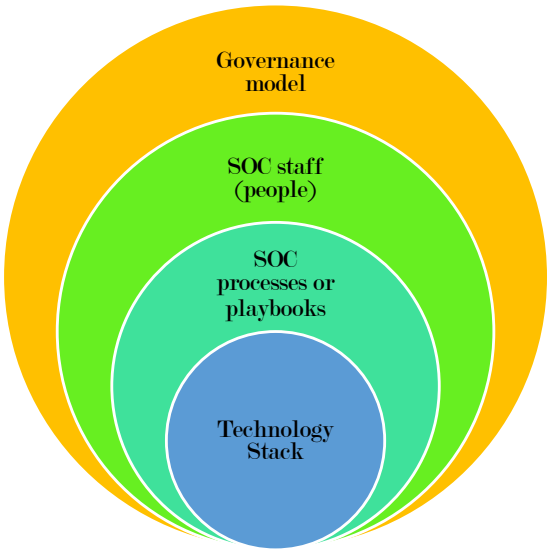

Figure 1.1: SOC Components

As we discuss later in this book, many operating models are used in industry depending upon needs of a particular organization.

1.1.1 What is a Modern SOC?

A modern SOC goes beyond dealing with detection of known threat and responding to incidents. It not only supports emerging technologies but also uses these technologies to improve SOC performance. A modern SOC implements all or a subset of the following:

- Includes physical security in the scope
- Integrate monitoring of Operational Technologies
- Use data analytics and machine learning for detection of previously unknown threat
- Subscribe to threat intelligence and potentially use a *Threat Intelligence Platform* or *TIP*
- Automate routine tasks for improving efficiency and speed of incident handling
- Close collaboration with broader IT teams as well as business leadership
- Build a learning culture for SOC staff to be continuously up-to-date about emerging threats

- Share knowledge and intelligence both inside the organization as well as with trusted industry forums and partners
- Integrates threat detection for emerging technologies
- Contributes to developing policies and standards to make SOC integration as part of project management and software delivery lifecycle

With the increased focus on protection of data and critical systems, skills development to manage a SOC are also becoming more and more challenging. A breadth of knowledge in many different areas is required to be an effective SOC analyst.

1.1.2 SOC Functions

A SOC is part of an overall risk management program and serves some basic functions as listed below and shown in Figure 1.2.

- Collect and manage logs as well as other useful telemetry data
- Gather intelligence on threat actors, attack methods, and indicators of compromise
- Analyze available data and create/rank alerts based upon risk to the organization
- Promptly respond to security incidents and minimize impact of incidents on business

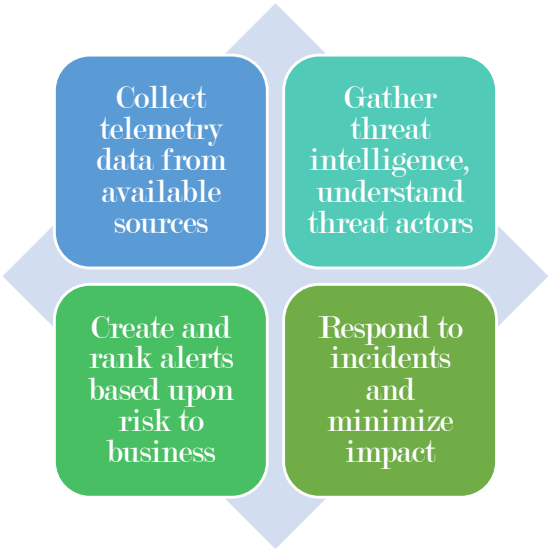

Figure 1.2: SOC Functions

To keep focus on success of core business and to optimize cost, many organizations outsource some or all of these functions to security vendors. Only very few businesses opt to completely manage an in-house SOC.

1.2 Purpose: Why Build SOC?

Before you embark on the journey of building a SOC, establish the purpose of SOC and have the business leadership agree on it. The *purpose* must be business driven instead of technology

driven. The purpose must answer the question: *Why do you really want to build a SOC?* The answer could be very different depending on the type of an organization. For example, a manufacturing corporation may need to ensure safe/smooth operation of plants, protecting intellectual property and manufacturing processes. On the other hand, primary purpose of a bank may be protecting consumer data and avoid financial fraud. A hospital may be worried about malware, ransomware, or protection against exploitation of medical equipment.

Some of the other areas of consideration are:

- Better risk management
- Fulfill compliance needs
- Business enablement
- Gain competitive advantage

In any case, establishing a clear purpose of SOC will help you narrow the focus of SOC, and better utilize investments.

1.3 SOC Business Models

There are three main business models for SOC, although there are number of variations within each of these models. These models are explained below.

1.3.1 In-House SOC

A completely in-house SOC is where an organization fully owns and manages operations of SOC. The organizations owns the technology and processes as well as hires people to operate the SOC. This is usually an expensive proposition and very few organizations have a business case to build and operate an in-house SOC. The size of the SOC may vary significantly depending upon the size of the organization and the scope.

1.3.2 Completely Outsourced SOC

Many organizations opt to engage a *Managed Security Services Provider* (MSSP) to build and operate SOC on behalf of the company. A major objective of this model is to benefit from experience of service providers, benefit from their established processes and get access to ongoing threat intelligence. Some companies buy or subscribe their own technology stack while others use technology from the service provider.

Typically, the organization still owns remediation tasks and participates in incident response in a completely outsourced SOC model.

1.3.3 Partially Outsourced SOC

In a partially outsourced SOC, some processes and technologies are owned by the organization while others are managed by a service provider (MSSP). A common example is outsourcing forensics and log analytics while keeping ownership of incident response and remediation. However, there are large number of variations in this model depending upon which components of a SOC you would like to outsource and which ones to keep in-house.

1.4 What it Takes to Build a SOC?

Building an in-house SOC is a major undertaking and it is much more than just buying and installing software tools. A SOC is a combination of a clear business purpose, a technology stack, processes, governance structure, hiring and continuously training people, and maintaining executive support. Please keep the following in mind when you are embarking on a journey to build a SOC:

- You should always start with a clear business purpose and desired outcome for a SOC
- Defining clear scope is very crucial and most people stumble in the beginning by not doing so.
- Proper planning for SOC implementation can save significant trouble later in the SOC lifecycle
- It may take more than a year (may be 2-3 years) to have a completely functional SOC
- It is a significant financial undertaking and executive support is necessary
- SOC needs continuous improvement, so you have to plan for budget to support improvement tasks in overall operational cost
- Building SOC is much more than just technology or implementing a SIEM platform
- It would be a mistake to try to build all capabilities in-house. For example, you may need some capabilities very infrequently (e.g. deep forensic expertise). A prudent approach is to contract with your partners/vendors for some tasks that don't need day-to-day work.

A successful SOC will test your tenacity, persistence, coalition building skills, and getting things done through influence rather than authority as you have to work with broader IT teams.

1.5 SOC Implementation: Incremental or Big Bang?

Should one make a big comprehensive plan for implementing SOC in one go using waterfall methodology, or use agile concepts to make improvements over time? Arguments can be made in both ways, but you should consider that building SOC is usually a multi-year project. A big bang approach can be disaster in some situations whereas incremental approach can help you learn and fine tune your strategy over a period of time by taking smaller steps. I am always for building a complete and multi-year strategy but starting with a small scope.

You should always prioritize and divide your SOC roadmap into three to six months long sub-projects (the smaller, the better). Consider the most important aspects that need to be implemented in these phases to build scope of your sub-projects. These aspects may fall into multiple categories like the following:

- *Technical aspects* such as log sources that need to be added to the scope, or types of use cases that need to be created.
- *Organizational aspects* may matter in larger and diversified organizations. For example, you may want to include or exclude some business units from SOC scope for a particular sub-project.
- *Regional* scope in the case of global organizations is quite important. In the initial phases of SOC implementation, my suggestion is to focus on one region or country and then bring other regions under SOC scope. This will also help you deal with regional and country-specific laws and compliance requirements gradually.

- *Single or Multiple SOC* implementations are a consideration in the case of global organizations where it could be important to keep data in certain regions.

You may have other categories specific to your organization and how you plan to use SOC for risk mitigation. The idea is to create a structured approach for dividing the task of SOC implementing into 6-12 phases over a three year period.

1.5.1 Single Site or Multi-Site

Some large organizations may decide to start with a single SOC, learn and fine tune their approach, and then create regional or business unit SOC separately. There may be business reasons from budgeting perspective. A common organizational reasons is that IT and Security responsibilities for different business units are not under one management.

Another reason for multi-site SOC is 24x7x365 operations where organizations build multiple SOC in follow-the-sun model. I will cover multiple SOC implications later in the book in detail from the perspective of hiring people and scheduling.

1.5.2 Business Unit Coverage

Large size organizations have multiple business units that may belong to completely different industry sectors. To properly manage risk, they may decide to build SOC initially with a limited scope covering only high-risk business units. Once they have covered the high risk areas, then they may decide to add more business units in a gradual manner.

1.6 SOC Lifecycle Phases

Building SOC is not a one-time activity but a continuous journey. As mentioned earlier, you will start small, design and implement and then learn from SOC operations before moving to the next phase. Then you will improve based upon your experience and expand the scope over a period of time. Typical SOC lifecycle is shown in Figure 1.3.

Following is a brief summary of activities for each phase.

1. **Plan** phase is about defining SOC mission, scope, building business case, getting executive sponsorship, budget approvals, and defining business outcomes.
2. **Design** phase includes making decisions about technology stack, locations, logistics, network and connectivity, log sources, hiring people, defining processes, building partnerships with IT teams and so on.
3. **Build** phase is all about implementing your design, fine tuning few things as you discover new/additional options that you may not have considered in design phase, start collecting logs, creating use cases and testing alerts.
4. **Operate** phase starts when you have built and tested SOC technology as well as processes and move to the steady state processes. Here you will schedule personnel, respond to alerts, create reports, use metrics and measure performance of your SOC.
5. **Improve** phase is related to standardizing process, fine tuning technology stack, creating new use cases, automate routine tasks. This is all about getting the best out of SOC investment. The improve phases starts right after the operations and continues in parallel.
6. **Expand** phase is part of multi-phase part of SOC where you start small initially. For example, you may have only one business unit in the initial scope or may have a subset of

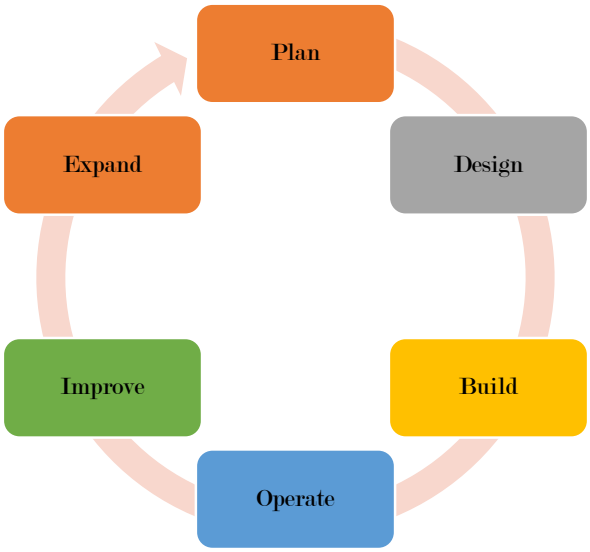

Figure 1.3: SOC Lifecycle Phases

log sources in the beginning. Once you have built some experience, then you will expand SOC to include additional areas of IT organization or add more business units, or going from local to global.

As you may have realized by now, SOC lifecycle goes into a circle. When you start expanding SOC in the *Expand* phase, you will get back to the planning and design and repeat the cycle. While the initial SOC implementation is a two-three years long project, continuous improvement and automation is an ongoing activity.

1.7 Who are the Stakeholders?

One may tend to think that information security is the largest, if not the only, stakeholder in setting up a SOC. However, that is hardly the case for numerous reasons. Not only most of the IT teams play their sole in building and operating SOC, non-IT teams like human resources, finance, legal, and public relations teams also need to be part of a comprehensive SOC strategy. Following is a short description of some of these stakeholders. More will be discussed later in this book.

- **The Network** teams play an important role. They are responsible for enabling SOC connectivity, segmenting SOC from the rest of the network, providing access to key data points like Netflows and full packet capture, and ensure that proper network capacity exists for collecting log data.
- **Server Infrastructure** teams not only provide support for key system in SOC but are also crucial to collect system logs, authentication data from identity and access management systems, among many other support items.
- **Human Resource** department plays key role in finding the right people for SOC staff, their training and retention.
- **CFO** and finance teams approve budget and embed SOC in corporate risk management

strategy. Without their support, realizing SOC budget could be a daunting task.

- **The Legal** teams provide support and cover for SOC activities that may result in legal issues (both internal and external) as a result of data leakages and breaches.

Building a coalition of internal teams and including them in SOC planning is, thus, crucial for your success. The sooner you start engaging them in a proactive manner, the better it is. Considering an inclusive governance board for SOC is always a great idea.

1.8 SOC Operations Time

Do you want to run Security Operations Center during the working hours, day time or round the clock? Your adversaries definitely don't follow your work hours, so you may want to think about your approach!

- **Business Hours** operation may include 8 AM to 5 PM.
- **24x7x365** operations, as the name shows, is for round the clock coverage.
- **Follow-the-Sun** model is still 24x7x365 operation but in this case you have multiple SOCs across the globe such that each individual SOC works only in the business hours of their respective region. However, when combined together, the SOC offers a complete 24x7x365 coverage.

More of this will be covered under section 2.7

1.9 SOC Stakeholders' Perspective

When building SOC business case, be mindful that people have different perspectives about SOC goals and objectives. Put yourself in the shows of the following roles and think how SOC will bring *value* to each of them.

- Business Executives
- Information Security Leaders
- Security practitioners
- Other IT teams including but not limited to IT, Network, Applications, Desktop and so on

There should be something for each team in the SOC plan.

1.10 Threat Modeling

Threat modeling is crucial task for planning and building a successful SOC. While this book is not indented to be a text on threat modeling, in simple words think about threat modeling as a practice to understand your adversaries, their methods to attack your organization, how you will identify the attacks and respond to these attacks. Threat modeling will help you define scope, determine interesting log sources, select appropriate tools and technologies and many other aspects to make SOC successful.

Many texts and online resources are available for threat modeling and my advice is to make it a standard practice to model and remodel threats. In the absence of proper threat modeling, you will end up wasting significant time, money and energy in collecting irrelevant logs and

investigating events that don't matter much. Threat modeling will also help you in creating appropriate use cases and filtering out noise.

1.11 Chapter Summary and Recommendations

Building a security operations center is a serious undertaking. It is prudent to start with collecting information, evaluating options and defining purpose of a SOC. It is crucial to answer a fundamental question: Why do you want to build a SOC? Once you have that question answered, then you can work on the following to build your understanding of different options:

- SOC business models (in-house, outsources, hybrid)
- SOC operating models (business hours or 24x7x365, follow-the-sun, single or multiple SOC)
- Understanding SOC lifecycle
- Phased approaches
- Understanding stakeholders
- Executive sponsorship
- Who could be part of SOC governance team?
- Building a business case
- Implementation plan
- Acquiring technologies
- Hiring and staffing

A well-thought out approach about the above will provide the base for a successful development of business case followed by the design and implementation.