Sisargo Publishing

Cybersecurity Arm Wrestling

Winning the perpetual fight against crime by building a modern

Security Operations Center

DRAFT VERSION

Rafeeq U. Rehman

August 11, 2019

Contents

List of Figures

Preface

This book has been a work-in-progress for quite some time and it looks like it will stay the same. Reason? Cybersecurity is a continuously evolving field and despite continuous efforts by the industry, there is no silver bullet to take care of emerging threats. Public and private sectors have build Security Operations Centers (SOC) either in-house or outsourced to security vendors, but many of these efforts don't bring the intended results. This is an effort to learn from experience of many people, research, practices that people have found useful and avoid common pitfalls in building SOC.

Cybersecurity is a Perpetual Arm Wrestling

People in Cybersecurity roles understand that it is an unending was between security professionals and their opponents with varying interests, mostly financially motivated [3]. New vulnerabilities are continuously discovered, new technologies are developed, and attackers are innovative in exploiting flaws to gain access to information assets for financial gains. It is fine with attackers to succeed only few times whereas the security professional tasked with defending businesses have to succeed all times. In essence, you are continuously trying to defeat your opponent. Hopefully you win this *perpetual arm wrestling* most of the times, but keep in mind that sometimes you will lose as well. You work on incident response preparation for those situations.

Book Audience

Security Operations Center (SOC) plays a key role in this perpetual arm wrestling to ensure you win most of the times. People, who are part of SOC planning, architecture, design, implementation, operations, and incidents response will find this book useful. Even if you are an experienced SOC professional, you will still find few interesting things as I have done significant research and interviewed many SOC professionals to include tips and to help avoid pitfalls. This book is also a window into my experience of last eight years in helping businesses of all sizes build security operations centers.

- **CISO** will benefit from chapters related to planning, business case development and budgeting information.
- **SOC Architects** - People who are responsible for designing and building security operations center will learn from this book about how to design SOC and avoid pitfalls.
- **Security operations staff** - The security operations team will be able to benefit from information related to job roles, 24x7x365 staff scheduling, training, building knowledge base and

other areas related to SOC operations.

- **Security Leaders** - Understand budgeting, metrics, dashboards

Insights presented in this book will be beneficial for all information security professionals.

Purpose of Book

This books is written with following key objectives in mind:

- Understand what it takes to build a SOC, both from financial and people perspective
- Decide which SOC model works better for you (insourced, outsourced, or a hybrid)
- Make your SOC project successful and avoid pitfalls
- Learn from experience of others
- Help you improve any existing SOC
- Cover emerging technologies and threat intelligence

Book Organization

The books ir organized in three parts and multiple chapters in each part. The book start with introduction and development of business case and then move to building and operations of SOC. The last part of the book is about continuous improvement of SOC over a period of time. Following is a brief summary of three parts.

- **Part I - SOC Planning**, covers introduction to SOC, building business case and budget
- **Part II - Building SOC**, covers everything from architecture, building and operations
- **Part III - Continuous Improvement**, is about governance and continuous improvement including threat hunting and meaningful metrics

Getting Latest Copy of Book

This book is available in both electronic and print formats (draft versions only in PDF format). The plan is to update the book on yearly basis to ensure all latest developments are covered. Always check for the latest version of this book on my personal blog site rafeeqrehman.com or at sisargo.org.

Your Feedback and Comments

Your feedback is important to me. Send your comments on my blog site rafeeqrehman.com or direct message on Twitter handle @rafeeq_rehman.

Part I

SOC Planning

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

A Chinese proverb

— Will I get unlimited supply of Mountain Dew?

Overheard in a SOC planning meeting

1 Introduction

Protecting confidentiality and integrity of data as well as availability of 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, automation and others are becoming crucial for business success, concept of a modern SOC is also going through an evolution process 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. 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 automation and 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 and organizational assets by continuously monitoring emerging threats, security events, analyzing and prioritizing these events, and responding to security incidents.

Typically a SOC consists of:

- ***Technologies*** for collecting log and other types of data, storing, and processing/analyzing

data. Main technologies used in SOC include Security Information and Event Management (SIEM) tool, log collection, ticket/incident management, forensic tools, and vulnerability management tools. SOC may also rely on other IT systems like asset management, change management, etc.

- ***People*** with different level of expertise in diverse areas including 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 management is a key process for success of every SOC.
- SOC ***governance*** structure

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

1.1.1 What is a Modern SOC

A modern SOC goes beyond dealing with known threat detection and response. 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:

- Integrates emerging technologies
- 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

With the increased focus on protection of data and critical systems, skills development to manage a SOC are also becoming more and more challenging.

1.2 What this Book is not about

The field of information security is evolving and responsibilities of information security leaders are expanding over time as I have been describing in CISO MindMap[1]. This book is not to cover all aspects of information security and has a very narrow focus on SOC. For example, this is not about how you will configure firewalls or IPS or proxy servers. Neither it is about establishing a

[1]See CISO MindMap at my blog http://rafeeqrehman.com

vulnerability management program or patching systems. However, we do use log data coming from security devices, system logs, and information from vulnerability scans in SOC operations (among other types of data). Basically we are focused on how to glean intelligence from a multitude of data sources, correlations, identifying interesting events and managing incidents. Everything else is out of scope of this book.

1.3 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 the type of an organization. For example, a manufacturing corporation may need to ensure 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 things you can think about 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 best utilize your monetary and personnel investments.

1.4 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.

1.4.1 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.

1.4.2 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 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.

1.4.3 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.

1.5 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 effort and resources 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 this initiative
- 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.

1.6 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.

1.6.1 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.

1.6.2 Business 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.

1.7 SOC Lifecycle Phases

Building SOC is not a one-time activity but a continuous journey. Typically 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 1.1.

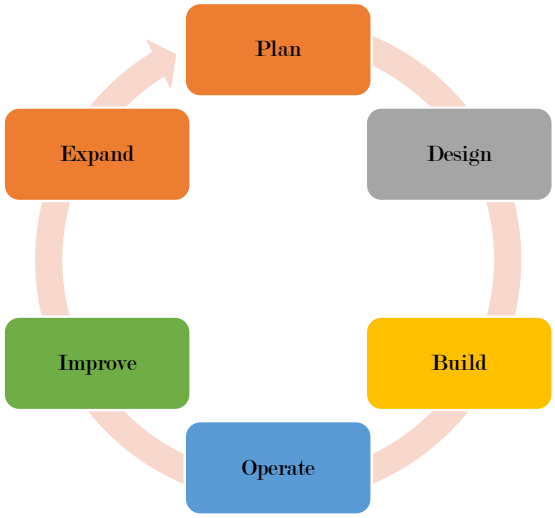

Figure 1.1: SOC Lifecycle Phases

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 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 that 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 so on. While the initial SOC implementation is a two-three years long project, continuous improvement and automation is an ongoing activity.

1.8 Who are the stake holders

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, 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.

1.9 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

1.10 SOC Goals/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.

1.11 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. Threat modeling will also help you in creating appropriate use case scenarios and filtering out noise.

1.12 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)
- Implementation options (single of multiple SOCs)
- Understanding SOC lifecycle
- Phases approaches
- Understanding stakeholders

- Executive sponsorship
- Who could be part of SOC governance team?

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.

"A business case captures the reasoning for initiating a project or task. It is often presented in a well-structured written document, but may also sometimes come in the form of a short verbal argument or presentation. The logic of the business case is that, whenever resources such as money or effort are consumed, they should be in support of a specific business need."

The Free Dictionary (tfd.com)

2

Business Case Development

Building a security operations center (SOC) is not a small task. It needs significant investment of money, time and resources. Like any other project, it should start with building a compelling business case. A typical business case includes many sections as outlined in this chapter. As it takes some time and many iterations to build a business case, you should always start working on it quite early. You can start with an outline of your business case using a template in section 2.15 and then modify as needed. As you work on building your business case, it is a great idea to get input from your leadership as well as few peers you trust the most.

The business case for SOC should include the following sections:

- Industry analysis
- Mission and goals
- SOC Scope
- Tools and technologies
- SOC location and space needs
- Staff requirements and management structure
- SOC operational plan
- Implementation phases
- Financial analysis
- SOC governance model

- Continuous improvement plan

A business case is a way to perform your due diligence and explore different options to achieve business goals. It is also a tool to get approval and funding for building SOC. This chapter addresses provides guidance and a template for building SOC business case.

2.1 Who is the Audience and Stakeholders?

Understanding the audience of SOC business case is key to proactively address their concerns and getting the plan approved. Typically there are multiple groups of audience for your business case. You have to speak to all of them, although in different parts of your business case. Some of these groups are listed below.

- **Executive Management** - this includes the people who are ultimately responsible for approving the budget. They need to understand business outcomes of SOC, financial analysis, return on investment, risk reduction, and which problem the SOC solves. The business case should clearly show why they should spend money on SOC and not on other competing projects. Remember, there are never unlimited funds and executive management always have to pick projects based upon the *value* each project brings to the business and shareholders.

  - CFO - Will write a check for the SOC and will expect some return on investment and reduction in risk.

  - CIO - Will sill support SOC activities through extended IT teams and would be interested in efficiency of operations, among other things.

  - Chief Legal Officer - Cover legal aspects of SOC when needed.

  Depending upon your particular organization, consider the C-level leadership and include how SOC project takes care of their interests.

- **Middle Management** - There are typically director level people who are looking for interests of their own departments and potentially competing with you for budget of their own projects. If you are able to tie SOC objectives with some of their objectives, you will increase chances of success of getting approval. For example, if SOC can provide analytics capability that improves IT troubleshooting, you can build alliance with your internal server or network teams.

- **Managers and IT Architects** - They have interest in how SOC will impact their daily life either positively or negatively. Will it make their lives easy or will it create extra work for them? Here you have to focus on making their work easy in terms providing timely information and incident resolution. You definitely want to avoid projecting SOC as something that can increase workload for other IT teams.

Each of these audience are looking for different things in the business case that caters to their specific needs and interests. You should strive to provide something for all stakeholders in your business case.

2.2 Why Build SOC

This is the most important and most difficult question to answer, but it must be answered. Unless you find a great answer, it would be a challenge to market the SOC internally and get funding. You will be challenged with comments like why we have to do it? Can't we live without it? Do other companies of our size and industry run SOC? How will it help business? And so on.

You have to bring all of your expertise together to find the best answer to this question: be a professor, a marketer, a business savvy professional, financial analyst, a risk manager, and a visionary. You can start collecting all reasons why a SOC is needed and then create your elevator pitch based upon what is the most important for your audience.

Consider ideas like the following:

- Risk Management?
- Compliance?
- Business Enablement?
- Competitive Advantage?
- Other reasons?

If you are working in a technology company, may be *business enablement* and *competitive advantage* are the most important aspects of your pitch. If you are in financial sector, overall *risk management* is always a concern.

Why is it important to answer the *why* question

Note that answering this question is not only necessary to create your elevator pitch, it is extremely important for you and the security team as well. This will provide a common vision to all stakeholders and will guide you through the scoping and planning phases.[19]

2.3 Building a Story

A compelling story adds significant impact to your business case. While discussion in section 2.2 will help you create your elevator pitch, the story will can be placed in the beginning of the business case document. A simple story can be built on the following steps:

1. *Where are we right now?* - Describe the current industry landscape, how security operations are managed within your organization, gaps, and risks.
2. *How the future looks like?* - Explain the future state and paint a compelling picture for your audience.
3. *Why we need to get there?* - Utilize your thought process for answering the the *Why* question in section 2.2

4. *How do we get there?* - Describe different options to get to the future state and the reason why you are choosing a particular path.

Building a story is an essential part of influencing stake holders where they understand what the future looks like and become enthusiastic in joining on a journey with you.

2.4 Business Case Sections

Depending upon your company culture, you may have a business case only few pages long or it may span 10-15 pages. Some organizations have specific templates for building business cases. Following are some sections that I would recommend for your SOC business case development.

Many times you would think that you are building business case for others. However, in my view developing a business case is beneficial for you more than anyone else. It gives you an opportunity to think deeply about your goals and the challenges you may face in this endeavor. So more than anything else, do it for yourself.

2.5 SOC Mission

Mission statement should be short and define clearly the purpose of SOC, incorporate the notion of *SOC customers*[1], what service it would provide and how these services will benefit SOC customers. If your mission statement is more than two sentences long, you should trim it down. A mission statement is something that you would memorize, put on a wall poster, and make it your video screen wallpaper.

2.6 SOC Goals

The goals should have a short list of objectives that you would like to achieve. I would suggest making goal list between three to five points. If you have too many goals, you may lose focus and dilute the purpose. Following are some examples of the goals and considerations that you may want to include but there could be others,more relevant to your organization.

- Goals related to revenue and cost
- Risk management goals
- Operational efficiency and speedy incident detection/response
- Corporate business goals and how SOC goals align with those

While defining SOC goals, keep in mind your audience. This is crucial part of your business plan. Setting ambiguous goals, or the ones that can't be measured or achievable, or the ones that are not relevant to your organization, will be a mistake. Many times people make mistake of setting lofty goals and use information security terminology that others are not able to understand.

[1]Customer is used as a generic term to define consumers of the SOC services. The customers may include internal IT operations, network, helpdesk, and others

Using SMART (Specific, Measurable, Attainable, Realistic, and Time-bound) method of setting goals is a good starting point. However, make sure that each goal you set is a *good idea* in the first place. You should go through multiple iterations of your goal list. Take feedback from other security professionals and use simple terms that people outside security can easily understand.

Once the information security team feels good about the list, take feedback from few key members of broader IT team who you trust. Make further iterations based upon their feedback.

Many SOC projects are multi-year long. It is a good idea to align your goal with each phase of the project. This will also help define scope of the project.

2.7 Defining SOC Scope

While defining SOC mission and goals are key starting points, defining SOC scope is crucial to manage the overall SOC project and break a large multi-year project into smaller phases. Break each phase further into milestones. This also helps in managing cost and simplify implementation. My suggestion is to divide a SOC project over multiple phases, each of which should be about six months long. Following are some key areas to consider when defining the scope of each phase.

2.7.1 SCOPE: Log Sources

Log sources vary widely, starting from security device logs, network components, applications, servers and many others. Collecting logs also needs significant investment in log storage and processing infrastructure. You want to prioritize log sources that bring the most value from security monitoring perspective. For these reasons, you should start with a small subset of log sources and expand the scope of log collection over time (in future phases of the project). While defining the scope of log collection for each phase, you can consider the following:

- Value of particular log source for identifying security events and detecting noticeable incidents (proactive).
- How a particular log source can help in incident investigations (reactive).
- Amount of log data that you can handle, both from analytics and storage perspectives.
- Compliance needs and requirements that a particular log source fulfills.
- Ease of collecting log data from a particular source.

Typically, you should start with logs coming from security devices (firewalls, IDS, content filtering and proxy servers, identity management systems, proxies, VPN concentrators, end-point detection and response systems, etc). The second preference may be server operating systems and public facing web server logs. Then you can move to applications, and so on. There is no prescribed order and you should define your own scope based upon your particular situation and which systems play a key role inside your organization.

With most of the organizations moving to Cloud, collecting logs from Cloud service providers like AWS, Azure, Google and others could become a priority for some organizations. Additionally, if you are using a Cloud Access Security Broker (CASB), collecting logs from CASB system in the initial phases of SOC implementation will also be a good idea.

For some manufacturing organizations, logs from IoT devices and operational technologies could provide significant value. Auto manufacturers could be interested in logs from connected vehicles.

You can also use threat modeling techniques to identify critical log sources and prioritize these accordingly.

2.7.2 SCOPE: Time of Day

Although everybody would like to have a 24x7x365 SOC but that is not always possible due to different constraints. An 8x5 (8 AM to 5 PM) or single-shift SOC may be a good starting point for many organizations, at least in the initial phases of SOC implementation. Once the initial phase is complete, you may want to add a second shift before going to a full 24x7x365 implementation. Global organizations may also start with a single SOC in one region and then use follow-the-sun model to achieve 24x7x365 coverage.

2.7.3 SCOPE: Business Units

Large organizations have multiple business units and all of these units don't need to be under SOC scope, or at least not in the first phase. While each organization may have a different criteria to identify which business unites to cover, some considerations may include:

- Criticality of a business unit for the organization.
- Type of data and privacy requirements.
- Compliance needs and local rules/regulations.
- Risk to brand as a result of large-scale security incident.

Selection of business units may also be phased approach.

2.7.4 SCOPE: Geographical Locations

Multinational organizations may decide SOC scope based upon preference of specific geographic locations, among other criteria.

2.7.5 SCOPE: Emerging Technologies

Fast emergence of new technologies including Internet of Things (IoT), blockchains, autonomous vehicles, drones, and others is also impacting security business. While this may not be the case for some, others may deem these technologies as business critical based upon their impact. Following are some technologies that you may want to cover in different phases of a SOC project.

- Machine Learning (ML), deep learning and other artificial intelligence related technologies.
- Internet of Things or IoT, collecting data from IoT devices, IoT botnets, identities and other aspects of IoT.
- Operational Technologies or OT that cover factories, industrial controls, SCADA systems.
- BlockChain

- Drones
- Autonomous vehicles
- Migration to Cloud

Your business is potentially provider or consumer of at least some of these technologies. You may also be interested in bringing these under SOC scope because you may be a service provider. In any case, threats to these and other emerging technologies are only going to grow as their deployment and use grows.

Following are few other areas to consider for SOC scope:

- **Incident Handling** - Demarcation of where incident response will be handed over to other IT/OT/Physical security teams and which parts will be covered by the SOC staff. This will also help in determination of who needs access to incident management application and be part of incident response team.
- **Incident Handling Support** - Which part of incidents will be outsourced to third parties, if any. For example, if the SOC does not include building in-depth forensic capability, it can be outsourced to a third party for major incidents.
- **Managing SOC IT Infrastructure** - SOC team manages security applications including SIEM and security tools. However, IT infrastructure is needed to run these applications and tools. Decide who will manage network, storage, server Operating System for SOC IT infrastructure. Who approves processes for incident handling when people outside SOC are involved in the incident response activities.
- **Connection with Outside Parties** - When outside parties like press, communication, law enforcement are engaged, decide who will establish relationships with these outside parties and manage communications with them.
- **Other Data Collection Scope** – What is the scope of data collections other than logs, including netflows, threat intelligence, physical security and so on. If Cloud environment is in the scope, what data can be collected from the Cloud Service Providers (CSP)?
- **Vulnerability Management** - Who manages critical vulnerabilities, from scanning to prioritization to patching.
- **Threat Intelligence Gathering and Use** - How threat intelligence will be gathered and utilized (internal or outsources/purchased).
- **Processes** - Define which processes will be part of SOC and which will be excluded. For example, is SOC responsible of education and awareness, pen testing, or patching? Depending upon organizational structure, these and other security operational processes may be part of SOC or outside of its scope.
- **Compliance** - What role SOC has in achieving and maintaining compliance with government and/or industry regulations.

2.8 Tools and Technologies

A major cost element of SOC business case is purchase of software/hardware tools and services. Other than log collection infrastructure, SIEM is a primary tool that almost all SOC implementations will use. Fortunately many Cloud based options are available where you can avoid capital expense on these technologies. Once again a phased approach could be very useful to kickstart your project such that you are making expenses on gradual basis.

Following is a list of tools to consider for purchase at different stages of your implementation plan:

- Log collection and analysis tools, including SIEM
- Vulnerability scanning and penetration testing
- Incident lifecycle management and ticketing
- Forensic and evidence collection
- Threat intelligence platform

In addition to core tools and technologies, you may have to rely on other IT teams for managing server infrastructure for SOC, desktops and laptops used by SOC analysts, networking gear, and other common IT services.

2.9 SOC Operations Management

From a day to day operations management perspective, there are three basic models that you can choose from:

- **Internal Management** - Your organization manages all SOC operations internally with your technology, by your people and using your own processes.
- **MSSP Management** - A Managed Security Services Provider (MSSP) that manages SOC operations with their own tools and processes while you collaborate with the MSSP for incident management and remediation.
- **Hybrid Management** - This is where you manage SOC but outsource some parts where you don't have or don't want to build internal capability for various reasons. For example, you may want to outsource forensics if this is done rarely and does not justify full time employees.

The operations management is a crucial decision and should not be taken lightly. In some cases it would make sense to keep the operations in-house whereas in other cases outsourcing may make sense. When building business case, make sure your focus on the *business outcomes* instead of owning a technology. The ultimate decision may also include considerations for compliance.

2.10 Staffing Needs

Main SOC staffing needs depend upon few key decisions like the following:

- Number of shifts, whether SOC is 8x5 or 24x7

- SOC functions kept in-house or outsourced
- Using internal infrastructure for SIEM or a Cloud service

You should consider number of people required for 24x7x365 SOC keeping in view vacation time, people getting sick or leaving company, weekends, and so on. Although collaboration with other IT and network teams can reduce staffing needs, the business case should not bet on that aspect as the SOC needs to stand and operate on its own.

2.11 SOC Logistics

Although it may seem trivial, you should not forget common logistics for building SOC. These include but not limited to the following:

- Location, rooms
- Furniture and lighting
- Desktops and laptops needed for staff
- Secure cabinets and other logistics for storage of evidence
- HVAC and environmental safety
- Any TV screens and signal to display weather, breaking news etc.

In the business plan, include these factors and make them part of financial analysis and budget requirements.

2.12 Budget and Financial Analysis

This section is the most crucial for your CFO and people who will approve the budget[2]. Some key aspects to consider and make your financial analysis more compelling may include:

- Take a phased approach and spread your budget over a period of time. Start small and then expand over 2-3 years.
- Ensure projecting return from SOC investments. The return may not always be in terms of money but could be in terms of risk reduction and efficiency.
- Think about taking advantage of existing technologies and open source tools.
- Separate capital costs from operational costs.
- Don't forget amortization and depreciation of capital goods.

Figure 2.1 shows a sample calculation for SOC budget. However, it is very simple and your calculations may be more complicated, taking into account multiple phases.

The finance people will pay attention to the terminology, so make sure you use the right financial terms and keywords they would be looking for.

[2]You can use a simple budget calculator spreadsheet from my blog site http://rafeeqrehman.com

Budget for Setting up SOC

SOC Budget Calculator Version 1, December 2016

Annual Personnel Cost Estimates

This is an estimate for 24x7 SOC with three shifts. Annual costs and number of analysts can change based upon your needs.

Job Item	Quantity	Individual Annual Cost	Total Annual Cost
Tier 1 Analysts	5	$80,000.00	$400,000.00
Tier 2 Analysts	3	$100,000.00	$300,000.00
Tier 3 Analysts/Threat Hunters	2	$120,000.00	$240,000.00
Forensic Specialist	1	$130,000.00	$130,000.00
Malware Engineer	1	$120,000.00	$120,000.00
SOC Manager	1	$140,000.00	$140,000.00
		Total Annual Cost:	**$1,330,000.00**

Capital Cost Estimates

Change the following costs depnding upon your own estimates. Consider these numbers as placeholder only.

Description	Quantity	Item Cost	Total Cost
SIEM Solution	1	$200,000.00	$200,000.00
Server Hardware	3	$100,000.00	$300,000.00
Laptops	13	$1,500.00	$19,500.00
Forensic Software	1	$40,000.00	$40,000.00
Secure Cabinets/Locks	1	$5,000.00	$5,000.00
Forensic Image Storage	1	$10,000.00	$10,000.00
Log Storage and backup	1	$200,000.00	$200,000.00
Office, Furniture, etc	1	$200,000.00	$200,000.00
Miscellaneous	1	$200,000.00	$200,000.00
Professional Consulting/design/setup	1	$100,000.00	$100,000.00
		Total Technology Capital Cost:	**$1,274,500.00**

Annual Recurring Cost Estimates

Everything below is an estimate. Change based upon discussion with vendors

Description	Quantity	Item Cost	Total Cost
Depreciation of office equipment			$0.00
Software/Hardware Maintenenace			$0.00
Staff Training, Skills update	13	5000	$65,000.00
IR Exercises	4	3000	$12,000.00
Threat Intelligence Feeds	1	10000	$10,000.00
Vulnerability Scanning (Network)	1	$40,000.00	$40,000.00
Vulnerability Scanning (Applications)	1	$30,000.00	$30,000.00
		Total Annual Cost:	**$157,000.00**

Grand Total

Following are estimated grand total costs (capital and annual recurring).

Grand total capital cost of establishing SOC:	**$1,274,500.00**
Grand total annual recurring cost for SOC:	**$1,487,000.00**

Figure 2.1: SOC Budget Calculator

2.13 SOC Governance Model

The SOC governance model is part of the overall security program governance. You should always for a governance committee and include key stakeholders to create governance framework. The committee is responsible for creating and approving SOC policies and processes, approve any changes to the existing policies and processes, and provide oversight to SOC activities. Figure 2.2 shows potential members of a SOC governance committee and its responsibilities.

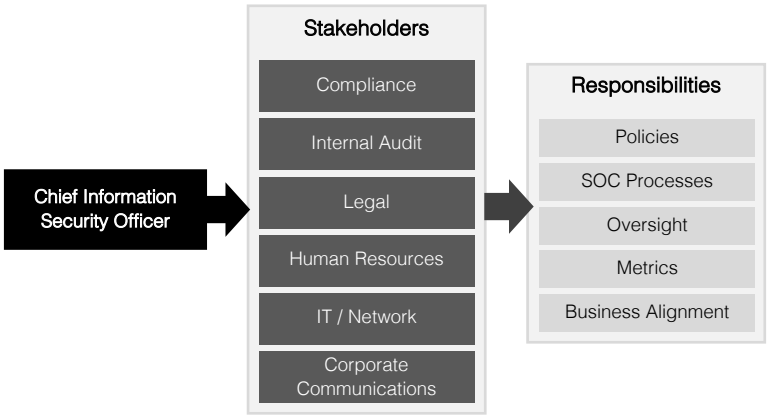

Figure 2.2: SOC governance committee and its responsibilities

> Please note that the governance committee is responsible for delegating authority to SOC to take certain actions and provide an oversight to ensure that SOC operations teams is using the authorization properly.

The governance committee should also perform regular audits of SOC operations, define/approve performance metrics, and review SOC performance on regular basis. It is also responsible to coordinate SOC improvement activities with broader IT teams and ensure that continuous improvement to SOC technologies and processes takes place. The committee may also require creation and review of annual reports. At the same time, the committee should also ensure that the oversight burden is minimal and kept in check.

While creating business case, it is a good idea to investigate potential candidates for the governance committee, their roles, and the value they will bring to the committee. You don't want to create a large group that may complicate the decision making process. At the same time, you don't want to miss a key stakeholder either. Also, make sure that members of the committee have appropriate authority to make decisions.

2.14 Risk Analysis

This may be a rather smaller section in your business case. You can address risk of building a SOC vs. risk of not building a SOC while keeping in view the following key areas:

- *Compliance Risk* - How this initiative will effect compliance needs?
- *Financial Risk* - Improvement in financial risk because SOC can lower probability of breaches or lower the impact of a breach. At the same time risk of losing money if the project fails.
- *Technology Change* - What if technology acquired for the project becomes obsolete or does not meet the needs of changing threat landscape? How can you lower this risk by using Cloud technology or use a managed security services provider who takes the ownership of technology risk?
- *Talent Retention* - For running SOC, you need to attract and retain qualified people. How would you manage risk of trained people leaving the organization?
- *Infrastructure Risk* - The underlying IT infrastructure risks are assumed with SOC. As an example, how would you plan for business continuity and disaster recovery.

Why Risk Analysis is Important?

A good risk analysis in your business case shows your due diligence in understanding risk scenarios and that you have a plan to mitigate or minimize risk associated with these scenarios.

2.15 SOC Business Case Template

Following are major sections of a SOC business case template.

1. Introduction and industry analysis
2. Definition of business problem
3. SOC mission and goals
4. SOC scope
5. Tools and technologies
6. Location and space needs
7. Staffing requirements
8. Operational plan
    - Governance structure
    - Policies and procedures
9. Implementation phases and milestones

- Year 1 plan
  - **Log Sources** - Security Logs
  - **Time coverage**
  - **Business Unites**
  - **Covered technologies**
  - **Tools and Technologies**
  - **Others**
- Year 2 plan
  - **Log Sources** - Security Logs
  - **Time coverage**
  - **Business Unites**
  - **Covered technologies**
  - **Tools and Technologies**
  - **Others**
- Year 3 plan
  - **Log Sources** - Security Logs
  - **Time coverage**
  - **Business Unites**
  - **Covered technologies**
  - **Tools and Technologies**
  - **Others**

10. SOC financial analysis
11. Risk Analysis
12. Summary and conclusions

2.16 Chapter Summary and Recommendations

- An exceptional business case is not only necessary to get approval and funding, it is also important for you to better plan the SOC.
- You have to wear multiple hats to build the business case, be open and transparent, and get input from different stakeholders.

- Going to management for budget without due diligence and without building a business case is a mistake.
- Building a business case without getting feedback from your superiors about corporate business strategy and lack of aligning SOC with the overall strategy is another common mistake.
- I highly recommend spending good amount of time on building SOC mission and goals and answering the *why* questions.
- Use template provided in section 2.15 as a starting point but modify it based upon your needs.
- Use diagrams in the business case, such as organizational chart, governance committee, etc.
- Always split your business plan in multiple phases so that you don't have to request a very large budget at one time.
- A sound financial analysis is crucial for the business plan. *Don't minimize* required funding as you may have to go back for extra money later on.

—Torture the data, and it will confess to anything.

Ronald Coase

You can have data without information, but you cannot have information without data.

Daniel Keys

3

Logs and Other Data Sources

Logs provide a wealth of information and that is one of the reasons almost all security standards and frameworks (NIST, ISO, PCI, and others) emphasize on collection, storage, and analysis of log data as one of the key component of any security program. Collecting and managing logs is a fundamental requirement of any SOC implementation and is needed to meet many compliance needs.

However, as we know, some log sources provide much more value to security programs compared to others. So while you can collect, store and process all data you want, thinking about the true value can help you create a more cost-effective and focused strategy.

A phased approach for log management is always prudent where you start with important, more valuable log sources first and then add additional log data as your program matures.

While traditional log collection using Syslog protocol and log files has worked for quite some time, newer technologies are bringing challenges to older log collection methods. With fast transition to Cloud based technologies, newer log data may come from SaaS[1] applications, Cloud application platform, server-less applications, IoT devices, operational technologies, connected vehicles, drones, smart city technologies, and many others. These new log sources don't always send logs with Syslog and may utilize APIs, web services, or Cloud services specially built for logging. While planning for collecting log data and building a log collection platform, all of these new options must be considered.

> Welcome to brave new world of log collection using many methods to collect logs from Cloud, IoT, Vehicles, Drones, Operations Technologies, and others. Standing up a Syslog server is not longer sufficient.

[1] Software as a Service

This chapter is to explore basic logging concepts, log sources and prioritization of logs, and building a simple and scalable log collection architecture.

3.1 Distributed Log Collection

A distributed log collection architecture where local log collectors receive logs from different log sources and then forward to one or more central locations is commonly used today. This architecture helps in providing resiliency and reduction of loss of data in case communication link to central log collection becomes unavailable. Figure 3.1 shows one such arrangement.

A distributed architecture can collect as well as index log data locally and then make the indexes available to search requests. This may be necessary to meet certain regional privacy needs like GDPR[9]. However, one need to balance the flexibility and scalability of distributed log collection infrastructure and the cost of managing it. As an example, indexing logs close to edge is attractive but it can create additional overhead in terms of correlation, reporting, alerting as well as cost of managing indexes at multiple locations. Needless to say that like everything else in life, there are some compromises to be made here as well!

3.2 Log Structure

Although structure of log messages from different log sources may vary slightly, there are some common fields that are usualy part of every message. At minimum, this will include:

- Logs are usually a time-series data and contain a time stamp that shows when message was created.
- Source IP address or host name to identify source of the log. It does not need to be an IP address, though. For example, it may be a GUID (Globally Unique Identifier) for some log sources, a VIN (Vehicle Identification Number) for a car, and so on.
- Message body which could be a text string, and in some cases, binary data that could be converted into a text string by the system analyzing the message. The body itself may be divided into many key-value pairs for additional fields.

There could be other fields as well that include but not limited to message priority, the service or facility that created the message, message category and so on. Format of Syslog messages is defined in RFC5424 [10]. In some cases you may also prefer to use a gateway to convert different types of logs and then use Syslog as log transfer protocol for centralized logging.

> In some literature you may find term ”event” which is usually a single log entry that contains interesting information.

Different vendors of security devices provide information about structure of log messages created by these technologies. In addition to simple text strings, logs may also be in many other formats including:

- CSV files

- XML documents
- JSON formatted logs
- Logs in binary formats
- Application logs with custom log format

You may have to use a log parser to convert logs from a specific format to something that SIEM can understand for analytics purpose.

3.3 Building a Scalable Logo Collection Infrastructure

Building a log collection infrastructure that can scale as more log data is brought under SOC scope is crucial for long-term success of your project. A typical architecture includes one or more local log collectors at each location. These collectors have local temporary storage in case communication links are not available to temporarily store data. The log collectors should also be capable of collecting logs using multiple mechanisms including but not limited to Syslog, API calls, retrieving log files from individual systems and so on. Figure 3.1 shows a simplified diagram for a single site with one log collector forwarding logs to a central location.

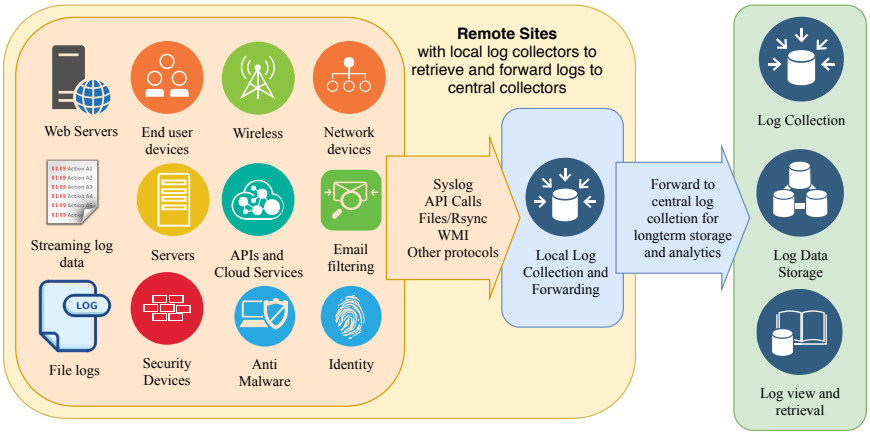

Figure 3.1: Building a scalable log collection infrastructure is crucial

Log collectors could be one or a combination of the following mechanisms. Specialized log collection mechanisms may be needed for modern log sources like connected vehicles, IoT systems, and others.

- A simple Linux machine running rSyslog [18] collector and forwarder
- Commercial log collectors that come with different SIEM solutions
- A windows machine that collect Windows logs and uses add-on software like Snare to forward these logs to a local or central collector
- A collector in Cloud environment such as AWS to collect logs using APIs and forward to central storage location

Syslog is a common and widely used protocol to collect logs over an IP network [10]. Typical log collection using Syslog infrastructure includes three roles as listed below [10].

- **Originator** is a system that is the source of log. It creates logs and sends it using Syslog protocol to a *Collector* or a *Relay*.
- **Collector** is a log receiver that collects logs either directly from the *Originator* or from *Relay*.
- **Relay** is an intermediate system that collects logs from *Originators* and relays these log messages to the *Collectors*. The *Relay* systems are used in large and distributed networks to collect logs at each locations and then send these logs to central log collectors.

The important aspect of log collection for a SOC project is that the methods and means should be standardized and documented for consistency purpose.

3.4 Selecting Log Sources

Some log sources are always important for security and are listed below:

- Security logs including firewalls, IDS/IPS. proxy servers, email content filtering, VPN servers.
- Logs from authentication and authorization sources like directories, domain controllers and other authentication sources.
- Web server logs, especially logs from public web servers.
- Security services hosted in Cloud (such as Cloud based URL filtering solutions) and SaaS (Software-as-a-Service) applications hosted in the Cloud.

Based upon a phased approach to log management, the collection process can be divided in a prioritized manner.

3.4.1 Approaches to identify valuable logs

One potential approach to selecting logs is to perform threat modeling. In this approach, you consider potential adversaries, their potential methods of attacking your organization and how these attacks will manifest in log data. Based upon this analysis you can make a selection of the most valuable log sources. As the results of this exercise may be different for each organization, it is necessary that all organizations perform their own threat modeling.

Another potential approach is to perform analysis on your most critical assets and identify log sources that will show an attack on these assets.

A third approach is thinking about utility of log in forensic investigations. In addition to logs that help identify malicious activity, some log sources may provide additional information and insights when you are investigating incidents. You may want to collect these logs as well and keep them for historical purposes. However, this should not be the first priority.

You can use Figure 3.2 as a sample table to score value of a log source to help prioritize it. Put an X in columns corresponding to each row if that column is relevant to that particular type of log

source. In the right-most column, put a score by counting number of X in the row. The highest scoring log sources should be priority for initial phases of SOC implementation.

Figure 3.2 is an example of prioritization.

How to Prioritize Log Sources

Log Source	Usefulness for threat detection?	Required for compliance?	Related to business critical application?	Valuable for forensic investigation?	Total score
DMZ Firewall	X	X	X	X	4
URL Filtering Proxy	X	X		X	3
Ecommerce Apache Server	X	X	X	X	4
Development Web Server WAF				X	1

Figure 3.2: How to prioritize log sources based upon usefulness

3.4.2 Using a phased approach

Whichever method you choose, you will always have more log data than you can effectively utilize. Make a selection for initial phase of your SOC implementation and then use a phased approach to bring more logs as your SOC become more mature and you are able to do something useful with the data you are collecting.

3.4.3 What to do with logs?

Typically, you will build use case scenarios in your Security Incident and Event Monitoring (SIEM) system and create alerts and incidents based upon these use cases. Although some logs may be collected only for forensic purposes, it would be wise to use maximum number of available log sources in creation of use case scenarios.

3.4.4 Log retrieval and search

Most organizations keep only a small subset of data online and archive historical log data. An important aspect is that logs should be readily retrievable from any archive when you need them for investigations and be collected at a central location. While selecting your tools, also consider quick search capability.

3.5 Security Log Sources

Technologies used to perform core information security tasks yield the best log data for threat detection and response. Collecting log data from these sources should be the first priority. Some of these technologies are listed below. While we do understand that every organization may not have all of these technologies implemented, you can easily start with these as your first phase of log collection.

- Network Intrusion Detection and Prevention Systems (IDS/IPS)
- Host based IDS
- Firewalls
- Proxy Servers
- VPN Concentrators
- Web App Firewalls
- Endpoint protection systems
- Data Loss Prevention (DLP) systems but be careful to handle sensitive data that may be in DLP logs
- Email/SPAM filtering
- Identify and Access management (IAM) Systems. Many organizations use Windows Active Directory domain controllers as part of identity management and these logs can be crucial. On the other hand, if you are using a Cloud based IAM system, make sure your Cloud identity provider is able to provide log collection option.
- Distributed Denial of Service (DDoS) technologies are mostly hosted by your Internet Service Provider (ISP) and could be useful in certain scenarios.
- Public Key Infrastructure (PKI) Systems
- Antivirus / Antimalware
- Cloud Access Security Broker (CASB)
- PKI (Public Key Infrastructure) systems

As many of these technologies are moving to Cloud, make sure logs are collected from Cloud technologies in addition to on-premises systems.

3.6 Server and System Logs

Server logs provide key insights for threat detection and response. First of all, make sure you start with collecting logs from servers used in the SOC itself. After that consider log collection from other servers based upon criticality of applications running on these servers.

- Windows

- Linux
- UNIX/Other
- Mainframe etc
- Virtualization technologies

3.7 Application Servers, Middleware and Business Systems

These are critical for business operations and provide a window into both employee and customer data. Attackers are mostly interested in getting access to these systems, enabling them find business data and exfilterate it. Following are some examples of servers or systems that you may be interested in getting logs from:

- Apache web server
- Other Web Servers and Application Servers
- Ecommerce Systems
- Databases
- Message Queues
- Order Management
- HR Systems
- Configuration Management Systems
- Business Applications
- DevOps systems, deployment servers

In most scenarios, you don't have to collect logs from all of these systems in the initial phases of your SOC implementation. However, logs from Ecommerce web servers, for example, may be crucial for threat detection and response.

3.8 Netflow

Netflow is a UDP protocol designed for collecting data about network traffic. Typically, routers collect netflow data and forward it to a netflow collector system. This data can be used to identify network traffic anomalies, command and control (C&C) traffic, and anomalies using machine learning algorithms. Netflow data provides excellent value for forensic investigations.

3.9 Applications

Log data from applications is challenging to handle for variety of reasons. Typically applications logs are not available, or the right type of logs are not available. The logs that you do get usually don't following standard conventions so you may have to write special log parsers. However, in

some cases these logs could provide significant value or may be required to meet compliance needs. Consider the following categories when evaluating usefulness of application logs:

- Commercial Applications - You are limited by the log data generated by the application. You also have to work with the vendor to get information about log format.
- Home grown applications - These are relatively easy as specific data can be logged by modifying the code. However, that will require additional expenses in development cost.
- Cloud applications - Most of the Cloud based applications do provide logging but retrieval of these logs may be a challenge.

Investigate log formats and how to ingest data into SIEM technologies.

3.10 Cloud

Almost all businesses have a Cloud strategy as the push for moving applications to Cloud continues. Logs from Cloud environment are very crucial for threat detection and response capabilities as ultimately it is not the Cloud provider who is responsible for protecting your data in the Cloud but you! When considering Cloud data, think about the following:

- Log collectors options provided by your Cloud vendor. Some Cloud vendors may provide raw log data using shared storage while others may use APIs to enable you collect logs. It is crucial to understand all available options and which of the options will work best for you. It may be a combination of multiple options depending upon how many Cloud vendors you use.
- The type of Cloud service also matters. Log collection for Infrastructure as a Service (IaaS) vendor may be different than a vendor who is providing you Software as a Service (SaaS) Cloud. For IaaS Cloud, you can typically collect logs for all layers of the IT stack whereas in the case of SaaS, you may get only application logs.
- In many IaaS services, you can host virtual security devices (VPN, FIrewalls, etc.) inside the Cloud. Collecting logs from these devices is as crucial as collecting logs from other security devices inside your corporate network or corporate data centers.

Many organizations have started implementing Cloud Access Security Broker (CASB) solutions to add an extra layer of security between corporate data centers and Cloud service providers. CASB logs should also be considered in the initial phases of SOC implementation.

3.11 Internet of Things (IoT)

Some industries are implementing IoT technologies more rapidly compared to others. IoT security is a topic in itself as these technologies bring new aspects that are not part of traditional network and IT security. These aspects include, but not limited to, different network protocols for IoT devices, security of firmware updates/consistency, non-interactive authentication and authorization, and so on. If IoT is a crucial part of your business, you should prioritize collecting and processing IoT logs appropriately.

3.12 Mobile and Handheld Devices

If your business manage mobile and handheld devices, you may be using a Mobile Device Management (MDM) system. Typically forwarding logs from MDM to centralized log collection systems is first good step for managing mobile device security.

3.13 Operational Technologies (OT) SCADA/ICS

Operational Technologies (OT) are mostly relevant in industrial environment, oil and gas sector, power generation and transmission. This requires a different skill set and in many cases OT SOC is managed separately. However, with IT and OT convergence in many industries, a modern SOC is really a converged SOC that handles both IT and OT environment. OT logs are coming from Programmable Logic Controllers (PLCs), Industrial Control Systems (ICS), Supervisory Control And Data Acquisition (SCADA) systems etc.

When dealing with OT logs and OT related incidents, make sure that SOC personnel are trained on OT systems as security considerations for OT are not exactly the same as general IT systems. Availability and safety are more important in OT world compared to confidentiality in the case of IT systems.

> Data from sensitive networks can be collected using technologies that allow one-way data transfer at the hardware level such that there is no way to reach back to the sensitive network. In general, these technologies are called "data diode". If you want to enable data collection from the OT network but also want to make sure there is no reverse path, please consider use of data diode hardware.

3.14 Physical Security Logs

Depending upon needs of your organization, physical security may be crucial and log data from physical security systems may be valuable for SOC. If the SOC scope includes physical security, identify all logs sources from physical security systems and prioritize them based upon their overall value. You may have to write special use cases and alerts for physical systems security and a different type of incident response plan.

3.15 Logging and NAT

In many networks, Network Address Translation (NAT) is commonly used for different reasons. NAT enables altering source or destination IP addresses during data packet's journey through the network. However, this may create serious issues for log collection infrastructure and to identify the true source of log data. If log sources in your network are behind a NAT router, make sure you find means to overcome his issue. Different log collectors, relays, and forwarders have the capability to overcome the NAT issues. RFC 1918 [11].

3.16 Logging and Network Time Protocol

A timestamp is an essential part of each log event. An important factor in building logging infrastructure is to ensure time synchronizing among all log sources to keep proper order of logs, necessary for correlation. Network Time Protocol (NTP) is commonly used for purpose. While NTP is a topic in itself, it is sufficient to at this point to understand that no logging infrastructure is complete until NTP is implemented to support it. Without it, log correlation and analytics will not work properly as logs are a time-series data.

Timestamp is a necessary part of log data to understand what happened and when it happened. Network Time Protocol (NTP) [15] [6] is a key protocol to keep time on all log sources synchronized. This is crucial to ensure that all logs can be placed in a chronological order when collected from a number of different sources.

NTP is a client-server protocol where the server is a standard time source and clients synchronize their local clock with the server on continuous basis. Many standard NTP servers are available on the Internet [14] and you can setup an internal NTP server that takes its time from the standard time sources.

3.17 Logging Standards

Lastly, building logging standards to identify type, amount, and level of logging also goes a long way to build a consistent approach throughout an organization. A logging standard must address requirements for logging at different levels including system, middleware, and applications. The logging standards should also specify accepted logging protocols, storage and lifecycle of log data. Logging standards must be updated at least on annual basis to ensure new sources and types of important logs are taken into consideration based upon their value.

Processes and standards for log collection play a crucial role for adding new log sources. There should be defined roles and responsibilities about who manages log sources and ensures logs are being forwarded, the types of logs that should be forwarded, any log collection agents needed for collecting log data, and so on. These standards should be part and parcel of overall SOC operational processes.

One common issue with log management is detection of missing log data. Sometimes, a server would stop sending logs due to a change applied to the server. In other cases updates to firewall policies may be the culprit where a port used for sending log data is accidentally blocked. A mechanism should be put in place to detect these situations and identify missing log data.

3.18 Chapter Summary and Recommendations

- A scalable log collection architecture and logging standards are necessary and foundational to build a successful SOC.
- You need to work with extended IT, network, and application owners to forward logs from a diverse set of systems. You also need their help to deploy and manage logging infrastructure (forwarder, relays, collectors).

- There are always more logs than you can collect and use in productive manner. This necessitates prioritization of logs based upon their usefulness for security monitoring and alerting. Use a phased approach to collect the most important logs first.
- You should always be mindful about the cost of log collection, storage, and processing. Many SIEM vendors license their products based upon the log volume and *collecting all logs* may become cost prohibitive very quickly.
- Many time, compliance needs mandate collection, storage and processing of specific types of logs from specific systems.
- Use of local log collectors that could help in reliability, buffering, compression and bandwidth saving.
- Use of NTP is crucial for getting correct log time stamps and proper correlation.
- Understanding that modern log collection needs support of diverse log collection mechanisms that include Syslog, APIs, IoT protocols like MQTT[16], plain text files, XML, binary logs and others.
- Build logging standards to bring consistency and clarity of logging requirements.
- A mechanism to detect missing logs must be part of log collection.

Part II

Building SOC