—SOC is a dynamic, fast paced, and stressful work environment. While tools and technology play an important role, the real key to a successful SOC is people with a positive mindset.

anonymous

7

SOC Operations and Incident Response

In Chapter 6 section 6.1, I introduced Plan-Design-Build-Operate approach of the overall SOC project[1]. While the previous chapters have been about the planning, designing and building the SOC, this chapter is focused on steady state operations, governance, and carrying out SOC tasks efficiently.

Note that the steady state operations phase starts when the *SOC project* is finished, marking the completion of SOC *build* phase. Later in this book, under Part III, you will learn more about continuous improvement and, potentially, SOC scope enhancements as part of your multi-phase plan. In some cases, you can have other parallel sub-project for improvements and enhancements.

What we cover in this chapter includes:

- SOC governance
- Human Resource management
- Incident Detection and Response
- Managing SOC technology infrastructure
- Build and Improve use cases
- Dealing with stress and SOC staff burnout
- SOC reporting and metrics
- SOC and meeting compliance needs
- SOC best practices and pitfalls

This chapter is the culmination of all preparations and work you have been doing in previous chapters, resulting in realization of the goal you started with. Now is the time to ensure that

[1]Well, there is *"Improve"* and *"Expand"* phases as shown in Figure 1.3 but we are not considering those phases yet!

SOC performs its functions and achieves its business objectives to quickly identify and respond to security incidents.

7.1 SOC Governance

SOC team needs alliances and cooperation across the business and technology organization. Building a governance model plays a key role in building these alliances, proper functioning and day to day operations of SOC. Often, a good governance model is closely tied to even getting funding for SOC [10]. A good governance model is also necessary for continuous improvements and building scope for future SOC enhancements and securing funds.

The governance model provides business leaders an oversight mechanism for SOC strategy, operations, review SOC policies and processes, and to continuously evaluate effectiveness of SOC. Failure to put a governance structure will significantly decrease probability achieving SOC objectives. The following part of this section highlights some of the activities that need to be part of SOC governance.

7.1.1 SOC Governance Board

The purpose of governance board is to provide oversight for SOC operations. Selection of member of governance board starts with identifying stakeholders. Section 1.7 on page 10 shows a list of usual SOC stakeholders. However, there may be additional stakeholders in your organization who would be your partner in success and should be included in the board. When creating a governance board, please ensure that following considerations are taken into account:

1. Create a purpose, mission and responsibility document for the governance board.
2. Include at least one member from each stakeholder team.
3. Schedule periodic meetings of the governance board with specific agenda. Agenda items related to performance reports of SOC should be part of every meeting.
4. The board should approve any change or update to policies and procedures of SOC.
5. The board should ensure that SOC is meeting its objectives. If not, the board should recommend corrective actions.
6. Collaboration with broader technology teams (or lack of it) should be discussed in regular board meeting.
7. The board should also advise on future direction of SOC scope and SOC expansion as well as continuous improvement.

As you can see from the above list, the governance board is crucial for the success of SOC operations and making any adjustments that are required from time to time.

7.1.2 Create Policies, Procedures and Standards

Development of policies, standards and procedures should be part of the project plan as mentioned in section 6.8. This basically means that a majority of policies and procedures should be ready before SOC enters into the steady state operations phase. However, that is always not the case. You may have some of these documents but these may be in initial phases of development. Even for mature SOC, you always need to review and update policies and procedures as part of regular governance process.

Table 7.1 shows a list of policies and procedures that are essential for running a SOC. While creating these policies and procedures, get help from overall corporate security policies and IT procedures to keep SOC policies consistent with corporate policies.

Category	List of Policies and Processes
Policies	• Change management policy • Incident management policy • Log management policy • Data encryption, storage, aging, and retrieval policies • Devices hardening policy • Vulnerability management policy • Business continuity and disaster recovery policy • Human resources policy • Threat intelligence gathering and use policy
Processes	• Change management process • Incident response process • Log management process • Incident identification, escalation and response process • Log collection process • Forensic process • Data storage, backup and retrieval process • Devices hardening process • Vulnerability management process • Business continuity and disaster recovery processes • Hiring processes • Managing operational shifts • Training and continuous development process • Threat intelligence gathering process • Threat intelligence integration process • Threat intelligence sharing process • Threat hunting process • Knowledge management process

Table 7.1: SOC Policies and Procedures

Keep policies and procedures simple and minimal so that each SOC staff member understands it. There is no need to write a PhD thesis that nobody fully understands, hence nobody fully follows.

When thinking about SOC processes, not only should you have good processes in place but also continuously evaluate process maturity and make continuous improvement. You can also take advantage from standards like COBIT, ISO 27K, ITIL and NIST to establish procedures.

While policies change less frequently, you may have to continuously learn from your operations and update your processes to make continuous improvements.

7.1.3 SOC Standards and Inclusion of Extended IT Teams

While many policies and processes would be used by the SOC staff, you should also create standards for the consumption of technology teams outside SOC. For example, infrastructure teams should know what are they supposed to do to enable logging for new servers or applications to be integrated into SOC. Similarly extended IT teams will be part of incident reporting and response processes. Some of the recommended standards for SOC are listed below.

- Log collection standards
- Incident identification and escalation standards
- Data encryption standards

If you have an internal GRC (Governance, Risk and Compliance) team, you can get help from their experts in creating effective policies, standards and processes.

7.1.4 Creating Process Flow Charts

Process flow charts are an effective way of creating a visualization of SOC processes. Swimlane charts enable you to add actors with process steps and decision making points. One of the advantage of creating process flow charts is that you can turn these flowcharts into posters that could be placed on walls for easy access to SOC staff and broader IT organization.

> Once you have created swimlane flow charts for a process, make sure to take it to SOC governance board for approval before broader distribution. In fact, all policies, standards and processes must be approved by the SOC governance board.

7.1.5 External Relationships (Law Enforcement and Others)

There are multiple reasons you want to have established relationships with law enforcement agencies in your area. First of all, you may be *required* to report some incidents and data breaches to law enforcement. Secondly, in some cases, law enforcement agencies may actually inform you about a breach if you are a secondary victim/target by threat actors who are acting against others. Third, in case of a large scale incident, you may actually need law enforcement as part of your incident response plan to investigate the incident. Fourth, in some cases law enforcement agencies may have capabilities that you don't have in-house and can help you fill gaps. Last, but not the least, some cases may end up in a court of law and these agencies could help you preserve the evidence such that it is admissible in courts.

For these and many other reasons, it is wise to establish relationships proactively so that you don't scramble to find contacts in the time of need.

You may also want to have some relationships with print and broadcast media, although it may be through your internal public relationship organization. These relationships are very useful when you want to communicate to general public or your customers in a meaningful and accurate manner as a response to a data breaches.

7.1.6 Coordination with other Teams

The SOC governance board should help in establishing relationships, interfaces, and processes for interaction with other teams. These relationships are not only needed for effective incident response, but are also required for other SOC tasks. For example, the SOC needs to be aware of any network changes, new applications, changes to existing applications, subscription to Cloud services, adding or removing servers or software etc.

- Other IT teams may add new log sources that you would be interested in.
- Change in any policies and procedures need to be coordinated with broader technology teams.
- You may need to make changes to SOC infrastructure that would require support from IT teams.
- SOC business continuity and disaster recovery processes are also closely tied to support from other teams.
- In many cases you may also need help from legal, HR, procurement and other non-IT departments within your organization.

As you can imagine, the list shown above is very limited and there are other areas where coordination is necessary and required and should be made part of SOC governance.

7.1.7 Service Level Agreements (SLAs)

SLA are used to measure efficiency of any operation, whether it is IT, SOC, or anything else. The SLAs are designed to maintain a certain minimum level of service that SOC customers (other teams) can expect from SOC. The SLAs are published and must be measured and reported and should have association with mission and objectives of the SOC [50]. You should also make sure that SLAs are reasonable so that SOC can actually meet but should not be too broad with no chances of failure.

Typical SOC SLAs include:

- SOC availability time and service hours.
- Time for incident identification to investigation.
- Time to escalation to CSIRT teams or incident responders.
- Mean time to resolution (MTTR).
- Mean time to onboard new log sources.
- Malware analysis
- Log retention and log retrieval

Note that in addition to SLAs for the SOC, you also need to make sure that any of your service providers also have defined SLAs and adhere to these. For examples, if you are outsourcing forensic or malware analysis to a third party, you must have SLAs signed with your service providers. If nothing else, you should have a support contract with your SIEM vendor that must include meaningful SLAs to make sure you get proper support when needed. When signing SLAs with your service providers, there should be a penalty when they fail to meet the SLAs.

7.2 Human Resource Management

From operations perspective, the main objective is to adequately man the SOC with appropriate number of analysts in different shifts.

7.2.1 Schedules and Shifts for 24x7x365 Operations

When doing my research on SOC operations and talking to experienced SOC managers and CISOs, I found that there are multiple ways different companies are trying to manage shift operations. Some of there are mentioned below.

- ***Nine Hour Shifts*** are used where 24x7x365 SOC requires that an analyst working in one shift get half hour of overlap time with the previous and next shift to transfer the in-progress work to analysts in the next shift. There are three shift in 24 hours with half hour overlap at the start and end of each shift.
- ***Twelve Hour Shifts*** work well in the scenario where SOC analysts work three days one week and four days the next week. This makes it easier to cover the weekends.
- ***Rotation*** is key to manage shift so that analysts are not stuck in one specific shift.
- ***Vacations and Emergencies*** require that SOC managers work proactively with SOC staff to stagger vacation time such that the service is not disrupted.

Building an environment to reduce stress levels, nourish cooperation, creating a team spirit, and providing tools and technologies to enable SOC staff work effectively are some other key aspects to manage schedule and shifts.

7.2.2 Daily Calls and Touch Points

Keeping all SOC staff updated with activities is obviously important as many of the daily actions may be closely related to each other. Taking a scheduled time to connect everyone and share quick updates is very helpful. This is even more crucial for 24x7x365 at the start/end of every shift as mentioned earlier.

7.3 Incident Response Process

Incident detection and response is the most crucial process of a SOC. We have already seen NIST recommendations for incident lifecycle management in section 5.8 on page 62. While building your processes, you can further segment activities shown in Figure 5.4. For example, *Detection and Analysis* may be further divided into *Detect* and *Analyze* steps. Essentially, there are these following seven steps that emerge from expanding the diagram in Figure 5.4.

1. Prepare
2. Detect
3. Analyze
4. Contain
5. Eradicate
6. Recover
7. Post incident activities

The important thing is to have efficient processes in place to quickly detect and respond to incidents and shorten a recovery time.

7.3.1 Incident Response Playbooks

Incident response playbooks are typically used to define step-by-step processes for handling different types of incidents throughout the lifecycle. The playbooks could be in graphical format like flowcharts or swimlane diagrams as well in narrative formats.

Playbooks should reflect incident response policy and processes "in practice". You should also have a relationship of playbook with different use cases such that when an alert triggers, IR teams can quickly figure out which playbook to use/follow.

Some example of typical playbooks for a SOC may include:

- Virus outbreak
- Phishing attacks
- Ransomware
- Denial of service
- Website compromise
- IoT

Each playbook should include all steps in the NIST incident response process (unless you are using a different incident response process). You can get help from many online resources to build playbooks [8][49][2][4][33].

7.3.2 Internal vs Retained Resources

Once in a while, you will have an unfortunate situation of dealing with a major security incident or a data breach. It may require additional help just because of the size of the response you need to mount or because some specific skill/expertise that you don't have in-house. For these, and other reasons, it is always a good idea to have a third party available for help, on a retainer basis.

So what should you look for in a third party while signing up for retainer services? Following are some considerations:

- Since attackers have no boundaries and incidents could be global in nature, make sure your incident response retainer provider has a global footprint, even if your business is regional or in one country.
- Also make sure they have people on staff who can speak major languages.
- Service Level Agreements (SLA) for providing services must be a key consideration. You want to make sure that help is available when you need it. Not a week after the incident.
- Also look for experience, history, and forensic capabilities of your vendor.

> Beware of zero-cost retainer services because to provide SLA, the service provider has to maintain a bench that costs money.

7.3.3 Setting up Computer Security Incident Response Team (CSIRT)

Where should SOC analysts or CSIRT team take lead and where should they collaborate during the incident response process? This section is a brief answer to this question and to establish a workflow.

Once SOC analysts declare an event as a security incident, the CSIRT takes the ownership of the incident, take necessary actions and close it. The objective of CSIRT is to execute workflow for responding to the incidents once it is escalated by SOC analysts. The main reason of having a CSIRT is to keep SOC analysts primarily focused on threat monitoring activities instead of getting into response activities which may take long time and may divert their attention away from their primary goal of threat monitoring and detection. A typical high level workflow for CSIRT team is shown in Figure 7.1 that also shows collaboration between SOC analysts and the CSIRT.

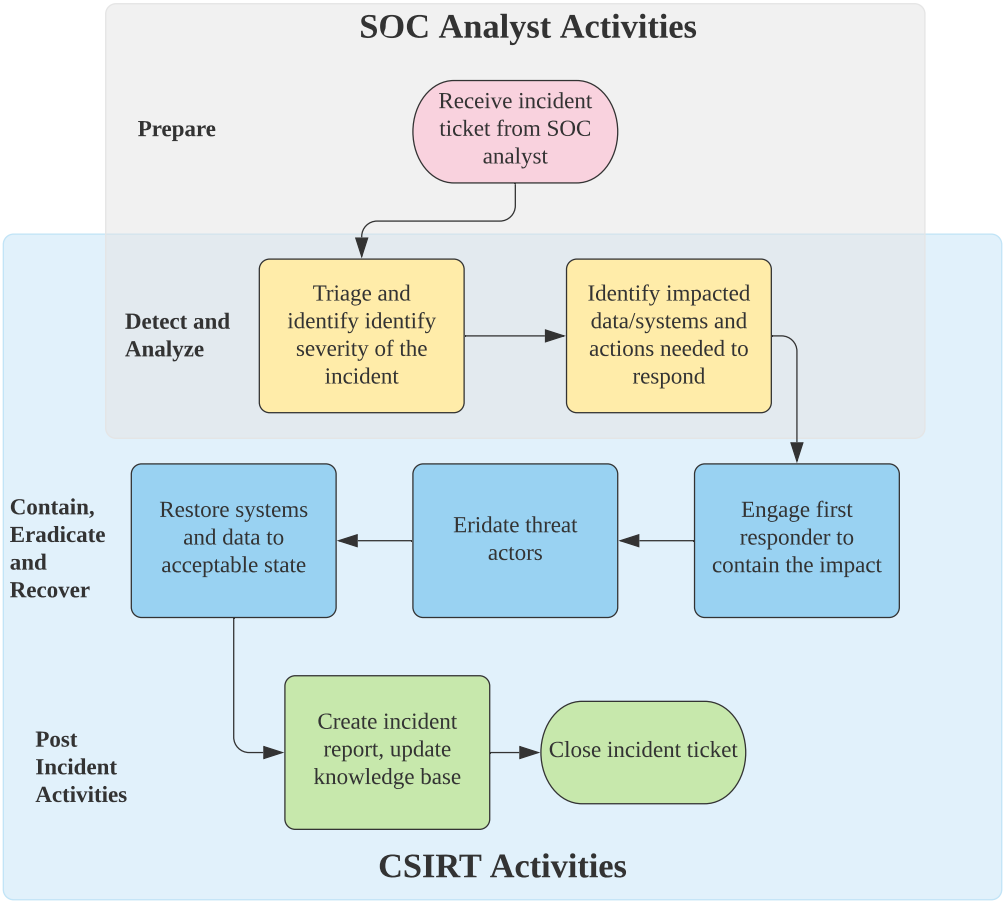

Figure 7.1: CSIRT Workflow

Note than the CSIRT team will be working with the SOC analysts in some phases of the incident response whereas it will take lead in containment, eradication, recovery and post incident activities. However, collaboration among all stakeholders is crucial during incident response and you should not strive for drawing hard lines for where role of one team starts/ends as long as the responders are clear about who is the lead on certain activities.

ENISA and other organizations have published good material about CSIRT establishment, training, and handbooks in case you need further help [14].

7.3.4 Threat Hunting

While majority of SOC work is reactive, starting with monitoring of activity and identifying threats in near-real time, proactive threat hunting plays a key roles in SOC success. Threat hunting helps discover threats that are not evident from log or other telemetry data. Threat hunters look for anomalies or other clues as a starting point, assuming that a breach has already happened, and search for threat activity.

> The objective of threat hunting is to reduce dwell time and mean time to detection.

Threat hunting could be initiated in a number of different ways:

- Threat hunters could take data from anomaly detection systems like user and entity behavior analysis (UEBA) and search for reasons of anomaly.
- Using indicators of compromise from threat intelligence feeds.
- Advisories from government or industry organizations.

Dark Web Hunting

Threat hunting is done both inside of your network as well as outside on the dark web. Experienced threat hunters are usually able to determine if stolen data is being sold/traded on dark web. If they find any stolen data, it gives them clues about when the data could have been stolen and what they need to look into to stop further bleeding.

Dark web hunting is also offered *as-a-service* by many vendors and could be a good option if you don't have internal threat hunters.

Threat Hunting with SOC Staff

Depending upon size of SOC team, you could have dedicated threat hunters or you could also use tier-III analysts for threat hunting when they are able to spare time.

7.3.5 Preparing for a Data Breach

Preparing for data breach is the best thing anyone can do for themselves and for their organization. Preparations for data breaches include many activities. If these activities are not led by the SOC team, SOC needs to be part of these at minimum. Examples of activities for data breach preparation are as follows:

- Provide breach response training to staff, including incident handling for insider threats.
- Building and testing incident response processes.
- Conducting breach simulation exercises on regular basis.
- Red team exercises to identify gaps in defensive controls.
- Building a first responder team and establishing a first responder training program.
- Budgeting for covering expenses of a data breach.
- Contracting with an incident response third party to help in case of a data breach.
- Purchasing a data breach insurance policy.

My suggestion is to create a quarterly schedule to test your preparedness for data breaches. You can use Table 7.2 as a starting point.

Quarter	List of activities
Q1	• Refresh training for data breach handling
Q2	• Data breach simulation exercises (internal) • Breach simulation for partners and supply chain (external)
Q3	• Red team exercise
Q4	• Review policies • Review insurance coverage and if it needs change in coverage

Table 7.2: Data breach preparedness testing

The data breach preparations should focus on the fact that sooner or later a data breach will happen and the organization should be ready to handle it.

7.3.6 Major Data Breach Stakeholders

Although major data breaches require a very coordinated response from all areas of the organization, typical major stakeholder are as follows.

- **Network** teams to monitor the network and make any changes during the response process.
- **Firewall Administrators** (and other security technology administrators)are part of incident response teams.
- **Desktop** management teams are also part of first responders, especially if endpoints are involved in data breach.
- **Server and Database** administrators
- **Legal** is typically involved in maintaining attorney-client privileges as well as evidence preservation for any litigation.
- **Human Resources** department may be involved during and after the data breach, especially when dealing with internal threat actors.
- **Public and investor relations** is always involved in effective external communications.

All major stakeholders should be part of preparations and exercises.

7.3.7 Major Activities as a Result of Data Breach Response

Following are some major activities that would occur as a response to data breach. It would be good to have people trained in these activities and making these part of your incident response plan.

- **Forensic and Investigation** - What happened, how it happened, who is behind it.

- **Evidence Collection and Preservation** - Major data breaches will follow law suites and evidence needs to be preserved so that it is acceptable in the court of law.
- **Law Enforcement Partnership** - Engage law enforcement agencies.
- **Compliance, Breach Notification and Public Relations** - When and who to send breach notification to, how to make public announcements.
- **Business Continuity and Disaster Recovery** - Ensure the business continues to operate. In some cases damaged systems may need to be recovered, for example, in the case of a ransomware attack.
- **Cyber Insurance** - Working with cyber insurance for claims.

So what you need to do? Think about the following:

- Create a liaison person for each team in broader IT organization.
- Convey incident response process with other teams and make them part of table top exercises.
- Establish a "first responder" team and train them on basic tasks like how to create image of a running system.

7.3.8 Forensic Capability

Some SOC organizations prefer to keep a base minimum level of forensic capability in-house and then contract an external vendor to provide additional forensic on as-needed basis. This strategy work well to manage cost as you may not need full time forensic investigator on a daily basis (if you are managing a small to medium size SOC).

7.4 SOC Technology Infrastructure Management

An essential part of SOC day-to-day operations is managing the technology that SOC relies upon. These may be infrastructure like network and servers, as well as applications and platforms. Just like other IT infrastructure, ITIL processes should be used for SOC infrastructure as well.

7.4.1 Change Management

SOC systems need changes and updates just like any other IT system. A change management process for SOC should address:

- Establish change management process following ITIL methodology. This process must be integrated into the overall IT change management process.
- Changes must be evaluated and approved before implementation. A backout option must be available for all changes.
- All patches to SIEM and other systems should be in the scope of change management.
- A special process for updating SIEM content, use cases and alerts should be established that ensure that all new alerts are well-tested and people are trained on what actions will be taken for new alerts.
- Always create a back-out strategy for changes.

If vulnerability management is part of the scope of your SOC, any changes to vulnerability scanning must also go through change management process.

7.4.2 Problem Management

ITIL provides specific definition for problem and recommendations for problem management. A problem is basically a recurring issue that need to be investigated to find root cause and then fix it. In SOC environment, recurring incidents of the same nature indicate an underlying problem in overall technology management. SOC staff should continuously evaluate incidents and find patterns that may point to a problem and then help solve it.

7.4.3 Business Continuity and Disaster Recovery (BC/DR) Exercises

Business Continuity and Disaster Recovery are essential of SOC planning and design as shown in section 6.7 on page 76. To validate and test BC/DR plans, you should:

1. Ensure BC/DR exercises are part of SOC policy.
2. Procedures are defined for conducting these exercises.
3. Exercises are conducted at least once a year. Twice a year would be better.
4. After each exercise, there must be a "lessons learned" meeting to identify required improvements.

The BC/DR exercises must demonstrate to meet recovery time objectives and recovery point objectives to be deemed as successful.

7.4.4 Patch Management

It would be better to leverage and follow corporate patch management processes for SOC. Most of the data breaches that leverage unpatched systems use vulnerabilities that are more than one year old [43]. While you don't want to be too aggressive, you don't want to be too slow either in applying patches to SOC systems.

7.4.5 Capacity Management

Telemetry data is even-increasing, new systems are added all the time, and businesses are expand their digital footprint. All of this results in increased requirements for SOC. Capacity management is essential to ensure SOC is ready to take and process additional data and provide additional services. A good practice is to plan capacity enhancements at least one year ahead of time and use SOC governance structure to prioritize and make budget requests.

7.4.6 Penetration Testing

SOC infrastructure should be treated as crown jewels of an organization and should be tested rigorously for any vulnerabilities and weaknesses. Penetration testing is a minimum control for this purpose. You should also perform periodic architectural review of SOC infrastructure to ensure any weaknesses are identified and fixed in a timely manner.

7.5 Build and Improve Use Cases

Building and improving "use cases" is a continuous task for SOC to identify threats. Section 5.4 on page 56 provides a detailed guideline for building use cases.

New use cases are developed and existing ones are fine tuned/updated as a result of situations like:

- After addition of new log data sources.
- As a result of new threat intelligence pointing to certain threats that may be of interest to your organization.
- To expand threat detection capabilities of SOC as part of continuous improvement.
- Reduce excessive false-positive rate resulting from poorly designed use cases.

In any case, SOC should have "content developer" role, either as a full time person or as part of tier-III responsibilities.

7.5.1 Identify Missing Log Data

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.

One approach for detecting missing logs is to create a use case specific to that purpose that monitors all important log sources, especially the one that are either high-risk or needed for compliance reasons. The use case would generate alerts when a log source stops sending data for a specific time period. The time period could be decided based upon the tolerance for specific items.

Another approach is to use some machine learning (ML) methods to detect missing logs as an anomaly and generate alerts. The advantage with ML methods is that it can learn/tune itself if you use unsupervised learning techniques.

7.6 Stress and SOC Staff Burnout

SOC staff is dealing with threats and investigations on regular basis every day. In many cases these threats are repetitive. Dealing with threats makes SOC staff stressed [28]. Stress and burnout are real problem and Thom Langford has written a blog about his personal experience as CISO coping with stress and its impact on his life which could be eye opening for many [30].

What is stress?

According National Institute of Health, MedlinePlus [32], *"Stress is a feeling of emotional or physical tension. It can come from any event or thought that makes you feel frustrated, angry, or nervous. Stress is your body's reaction to a challenge or demand. In short bursts, stress can be positive, such as when it helps you avoid danger or meet a deadline. But when stress lasts for a long time, it may harm your health".*

Chronic stress results in burnout of SOC staff. Burnout is a state of mental and physical exhaustion due to prolonged stress that drains out energy.

- Burnout is a result of constant stress. If you find a co-worker calling sick often or coming late to work, it may be a sign of burnout.
- Burnout may also manifest in an otherwise efficient person taking longer to finish tasks.

SOC manager should not only take care of themselves against these very real issues but also make sure SOC staff is healthy with a good work-life balance. I can't emphasize enough how important this is for a successful SOC.

PITFALL: Is stress and burnout real?

As part of my research for this book, I had the opportunity to talk to medical doctors to better understand stress, how it works, and its impact on performance and productivity of people. After these discussions, I am even more convinced that this is an area that SOC managers and CISOs must know about and make it part of overall SOC planning. Ignoring implications of stress not only has dire consequences on individuals' life but also impacts success of a SOC.

7.6.1 How to Identify if SOC Staff is Stressed Out?

SOC managers need to understand stress and take actions to minimize its impact on SOC staff. Every person takes stress differently while living through the same type of experiences. Prolonged stress results in exhaustion and results in visible signs of damage to one's health. If you see a co-worker agitated, frustrated, or overwhelmed, it could be first sign of stress.

7.6.2 What SOC Managers Can Do?

Well-being of SOC staff must be at the top of any SOC manager agenda. It is not only a good practice but is also essential for staff retention and operational efficiency of SOC. TO start with, managers must know:

- What causes stress and burnout?
- How to find if an employee is stressed out?
- What managers can do to address this issue?

One of the ways stress manifests in terms of physical health is hypertension. The research in this area is well documented and largely accepted [41].

Following are some actions that can reduce stress for SOC staff:

- Flexibility of working hours.
- Recognition of the work SOC staff does.
- Making sure staff takes time for lunch and take breaks. They are not too much absorbed in work such that they forget to take breaks.
- Reduce console time for staff, rotate their duties.
- Provide some time where staff can work on "things they like" or on "problems they want to solve".
- Since triage of events could involve performing the same tasks over and over, work on tools and automation to minimize fatigue from these repetitive tasks. If you have not yet, consider investing in SOAR tools.
- Make sure staff members take vacation and other time off.
- Celebrate successes, no matter how small they are.
- It may not be a bad idea in investing in buying gym membership for SOC staff.

I would strongly recommend that each SOC should encourage SOC staff to check their blood pressure on regular basis, which could be a sign of stress, especially for young people. To address privacy concerns, an option should be provided to staff to buy and keep a blood pressure meter at home. Decent personal use equipment costs less than $100 and is a good investment in SOC staff health.

Another general recommendation is to increase awareness of stress among SOC staff. One way to do so is to purchase few "stress posters" and place these on SOC walls as a constant reminder.

7.7 SOC Reporting and Metrics

Effective governance requires meaningful metrics and reporting. The project plan should include the following:

- Define a list of meaningful SOC metrics that show workload and effectiveness of SOC in achieving objectives (also means that SOC objectives should be defined in the first place!)
- How to automate data collection for metrics and avoid manual work
- Frequency for metrics and reporting
- Executive dashboards

The key to successful metrics and reporting is ensuring that these metrics and reports are meaningful and automated.

7.8 SOC and Compliance Needs

Almost all security compliance standards require log management, threat detection and incident response. Hence a SOC is always tied to compliance needs which the SOC managers need to fully understand to ensure successful audits. My suggestions are:

- Understand and list all compliance needs and section of standards/regulations where SOC has a role to play (e.g. PCI DSS).
- Get an agreement with internal compliance teams and/or auditors about what actions and reports they need to meet the compliance needs.
- Automate these reports and save historical copies.

The less time you spend on compliance, the better it is. A little upfront planning and automation will go a long way to achieve that goal.

7.9 SOC Integration Points

SOC does not live and operate in isolation and there are many integration points, not only from technology perspective but also for processes. Over the lifecycle of SOC, you will continuously be engaged in adding new integration as well as make the current integration more efficient. Following are some of the key areas that you should consider:

- New log sources
- Missing log detection
- Ticketing (could be internal as well as external)

- CSIRT teams
- Asset management
- Vulnerability scanning
- Crisis management
- Cloud providers
- External incident response retainer contracted firms
- Network Operations Center (NOC) as many incidents will require collaboration between NOC and SOC.
- Threat intelligence and information sharing, both internal and external to the organization.
- SOAR technologies (if these are part of your SOC environment).

7.10 Additional SOC Best Practices

This section is to list some of the best practices that are not discussed earlier in this chapter but would be very helpful in SOC operations.

7.10.1 Maintain SOC Runbook

A runbook is typically collection of procedures and operations that SOC staff carries out. It is also used to keep track of SOC staff activities, build workflows, and as a reference. Effective runbooks enable new staff members understand, troubleshoot and manage systems as well as handle exceptions/contingencies. You can have runbook as printed copies or in electronic form.

7.10.2 Create and maintain a risk register

A risk register is used to maintain a list of known risks, associated mitigation controls, risk owners, probability, and impact. As a starting point, you can use a simple table like 7.3 or created a more sophisticated one.

Risk	Owner	Rating	Owner	Probability	Impact	Mitigation Controls

Table 7.3: A sample (simple) risk register

7.10.3 Knowledge Management, Wiki

An internal Wiki or a similar system is necessary for SOC staff to document any new items they learn, workarounds, known issues and other knowledge items that would be useful for SOC staff. When staff work in shifts, they are not always able to meet each other and exchange information. Wiki becomes very helpful in maintain "tribal knowledge" and helps in resolving issues, especially for repeating incidents.

7.10.4 Staff Quality

Although you have a number of SOC analysts positions that you need to fill, but always prefer quality over quantity[51] even if you have to wait and even if it takes longer time to fill these jobs.

7.11 Chapter Summary and Recommendations

We have covered a lot of ground in this chapter as smooth and efficient operations is the most important part of any SOC. Following is the summary of crucial parts that contribute towards success of SOC.

- Importance of SOC governance can't be emphasized enough. This is the most critical success factor for long-term success.
- Hiring the right kind of people, training, managing their stress levels, and scheduling shifts is very critical as well.
- The most important process for SOC is incident detection and response. Building and improving use cases, automation and use of SOAR technologies is part of it.
- Applying ITIL processes to manage SOC infrastructure is quite important.
- Meaningful metrics, automated reports, and dashboards do help not only in meeting compliance needs but also facilitate effective communications across broader IT teams as well as business leadership.
- Last, but not the least, maintain a risk register, plan for next year, and always be ready to respond to data breaches.