Main Steps in Setting-Up a SOC Team

Authors: Theodor Adam, Florin Andrei, Larisa Gabudeanu, Victor Rotaru

Copy Editor: Alexandru Mircea Rotaru

Day by day, security threats are evolving in complexity and diversity. Right now, “no matter what business you are in, no matter what size your organization has, no matter where you are located, your business is at risk. And this risk increases day by day”. We already are aware that, in our age, information security prevention is no longer optional, and that security, and cyber defense in particular, should be high priorities.

The key to cyber defense today is to develop an organizational structure that continuously evolves in order to counter advanced attacks. This organizational structure is called a Security Operations Center (SOC), and relies on skilled security specialists, technology, and processes. The SOC’s goals are to prevent; monitor and detect; and investigate and respond to all types of cyber threats.

A Security Operations Center (SOC) is a functional unit specifically built to be the first line of defense for your organization. Therefore, its area of operation (AO) must be very well defined and should cover all equipment and applications used by the organization. This is the only way to assure a proper and effective protection against threats. SOCs are led by a SOC Manager or a Chief Security Officer.

SOCs perform the following key tasks:

1. Proactive Network Maintenance and Monitoring
2. Assessment of the Network Security
3. Incident Analysis
4. Threat Intelligence
5. Information Assurance
6. Information Security Compliance

7. Security Governance
8. SOC Support

One of the key elements of a SOC is a Security Information and Event Management (SIEM), a software solution that aggregates and correlates data from different security feeds across the monitored infrastructure. A SIEM performs proactive monitoring and analysis, and provides event correlation, alerting, and data visualization. Through these functions, it helps the organization detect and mitigate threats. Even organizations with limited resources can implement a SIEM, as there are many open source solutions available.

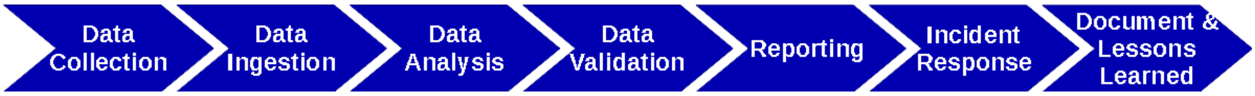

Figure 1. Typical workflow for Security Operations Center

1. **Data Collection** – Log data are collected from various sources / security feeds (devices, applications, etc.) on the network and sent to the SIEM;
2. **Data Ingestion** – Collected data together with threat and contextual data are ingested into SIEM to easily standardize casing of all fields parsed and produce security alerts;
3. **Data Analysis** – Alerts generated by SIEM are reviewed and evaluated on their urgency and relevancy;
4. **Data Validation** – Alerts triage is performed and incidents are validated;
5. **Reporting** – Validated incidents are escalated to response team through the ticketing system;
6. **Incident Response** – Incident Response Team reviews incidents and performs incident response activities;
7. **Document & Lessons Learned** – Document incident for audit purposes and lessons learned;

Without proper visibility and control over the entire infrastructure, blind spots can form in the network security posture. These blind spots represent a weakness in your defenses and may be subject to exploitation or entry points for ill-intended parties. This is why the SOC's goal is to gain a complete view of the business's threat landscape, including third-party services and traffic flowing between these assets.

Your SOC team is crucial regardless of what technology and applications you might implement as part of your SOC. Their level of expertise will determine how fast they will detect a threat and how fast they will identify, build, and apply a response. Considering the sensitivity of their activity, all SOC team members must be well trained, as their knowhow is critical to identifying and responding quickly to new threats, which is vital to your organization.

One of the main challenges to create a SOC is staffing. Finding skilled people and keeping them on board can be a nightmare for most SOC Managers. In a business context like information security, which demands high level of expertise, the competition goes beyond a company's profile. Let's face it: a company down the street in a different industry is still your competitor for talent. The evolving threats push you to continuously improve your security team's professional skills in order to keep them competitive fighting against threat actors. This is why training your security staff is a win-win business, and can become a differentiator that serves two purposes: getting better performance from the workers you have and showing those workers that you value them enough to invest in them. This creates employee retention as well. If you want more stability, which means less turnover, you need to offer them something that each of them values: training and professional growth.

The roles and responsibilities you should consider for your SOC are:

1. **Security Analyst** - Reviews the latest (SIEM) alerts to determine relevancy and urgency of identified events. Creates new trouble tickets for alerts that signal an incident and require Incident Response review. Runs vulnerability scans and reviews vulnerability assessment reports. Manages and configures security monitoring tools. Having a former white hat hacker experience is a big plus for this role.

2. **Threat Hunter** - Reviews asset discovery and vulnerability assessment data. Explores ways to identify stealthy threats that may have found their way inside your network, without detection, using the latest threat intelligence. Conducts penetration tests on production systems to validate resiliency and discover areas of weakness to fix. Recommends how to optimize security monitoring tools based on threat hunting discoveries. This is a senior security analyst role, which requires expertise in threat hunting.

3. **Security Engineer** - Maintains tools used, recommends new tools, and applies security updates for those tools. Designs and builds a security infrastructure and network security for an organization. Oversees the security architecture build over different systems.

4. **Security Manager** - Supervises the SOC team's activity. Recruits, hires, trains, and assesses the staff. Manages the escalation process and reviews incident reports. Acts as

Incident Response Manager when required. Develops and executes crisis communication plan to CISO and other stakeholders. Runs compliance reports and supports the audit process. Measures SOC performance metrics and communicates the value of security operations to business leaders.

Other roles you should consider for your SOC include:

5. **Penetration tester** - also known as "ethical hacker," is a highly skilled security specialist that uses different tools and techniques, attempting to breach computer and network security systems.
6. **Compliance officer** - ensures that a company complies with its outside regulatory and legal requirements, as well as internal policies and regulations.

There are two main responsibilities involved with the SOC team:

1. Maintaining security monitoring and analyzing your security on an ongoing basis. Detecting, analyzing, and responding to security incidents using a combination of people, processes and technology.
2. Proactively investigating suspicious activities to keep your infrastructure secure by ensuring that potential security incidents are correctly defended, identified, analyzed, investigated, and escalated.

Setting-up a SOC requires the following steps:

1. **Define a SOC strategy for your organization** – Defining a Mission and Vision for your SOC, along with defining the SOC objectives, will create, in a few sentences, the same understanding both within the organization and for external parties about the SOC implementation you lead;
2. **Define, approve and implement the organizational structure for SOC** - For a SOC to become operational, the designed organizational structure must be approved and implemented. Sometimes, this process can take months. Thus, your SOC might start off working using an interim structure, to enable work to progress;
3. **Hire and appoint staff** - The new structure must be filled with competent and skilled staff. It is highly likely that only a few positions will be filled with current staff; thus, additional staff members must be hired. You should consider that potential recruits often

lack the required competences, and you will need to give them some time and appropriate training to assure their professional growth;

4. **Preparation of facilities** - Facilities must be prepared by taking into account physical security and appropriate access rights - at least the security monitoring room should be protected from unauthorized physical access;

5. **Development and implementation of detailed processes and procedures** – Development and implementation of the SOC processes, policies and procedures; IT processes and procedures; information security policy; security controls; and procedures within SOC;

6. **Implementation of technology for the automation of processes** - Installing, configuring, documenting, and testing technologies for automation of processes within SOC;

7. **Define a training plan for different staff roles** – A yearly training plan should be defined for each role of the SOC team in order to assure the continuous improvement of their skills;

8. **Execute training for different staff roles according to the training plan** – Apply the training plan as defined. Further training can be carried out as planned. Skills gaps can be identified using crisis drills and blue-red teaming exercises;

9. **Signing of relevant agreements with the constituency, stakeholders and partners** - Ensure expectations and authorities of the SOC are well-defined and recognized from the start, especially by those in the SOC's management chain;

10. **Test run of SOC services and tuning of results** - Once the processes and technologies have been implemented, it is important to run tests for at least couple of days in order to identify any deficiencies in processes and technologies. Tuning actions should then be carried out for appropriate adjustments of the implemented processes and technologies;

11. **SOC Go Live** – Now your implementation of SOC is ready. You can launch your SOC into production and celebrate;

Conclusions

Building a SOC is a challenging endeavor. Successful implementation requires careful definition and planning. Do a few things well rather than many things poorly. The main focus of the SOC team should be on prevention by enforcing security policy and controls, as well as assessing and mitigating risks.

You need to ensure strong quality control for everything that leaves the SOC. You need to gain trust and credibility for your SOC implementation and SOC team as well.

Define KPIs and measure them on monthly basis in order to ensure the SOC services are delivered effectively, thus proving that your investment in SOC means money well spent.