CYREBRO

HOW TO BUILD A SOC: A COMPLETE GUIDE

TABLE OF CONTENTS

Introduction

The threat landscape is forever changing and the number of cyberattacks organizations face each year is forever growing too. As data breaches become more expensive, malware becomes more disruptive, and cyberattacks become more intricate, dealing with threats is now the job of a specialized Security Operations Center (SOC).

Instead of all security being handled by an IT team, SOCs are standalone security teams that are specialized in threat detection, security monitoring, and dealing with security events. They consist of setting up and operating war rooms that are populated with SOC personnel and effective security tools. According to Ponemon, **80% of organizations believe Security Operations Centers (SOCs) are essential to a strong security posture.**

A SOC is a necessity in the modern landscape, but they are not easy to set up and maintain. Cutting corners leads to serious security problems, so if you're thinking of building an in-house SOC, it's important to understand and make sure you have the key required elements. This guide will detail the steps it takes to build a SOC, so you can decide if the DIY approach is right for your business.

The Benefits of a SOC

Implementing a SOC has many benefits for organizations of all sizes, but while every organization doesn't necessarily need a fully staffed, 24/7 SOC that would rival a nation-state, there are key components that are required for all functioning SOCs.

Building a small-scale SOC is more than implementing threat detection and intrusion prevention tools. Organizations that cut corners will discover that threats will go undetected for longer and their ineffectual security practices will cost more than the results justify.

The Challenges a SOC-less Organization Faces

Before we dive into the reasons why your business is considering a SOC, let's take a quick look at the challenges faced when a business tackles cybersecurity without a security operations center.

An organization without a SOC can face serious repercussions. A company's incident response times are increased, security monitoring is inconsistent at best, and event management becomes a grueling task that is handled by a non-specialist. Research from IBM showed that $2.46 million was the total cost gap for organizations with incident response capabilities versus no incident response capabilities.

4 Challenges a SOC-less Organization Faces Risk Every Day

Slow responses to security events are inevitable in a SOC-less organization. Without a dedicated team that is analyzing events as they are logged, preventable threats slip through the cracks due to inconsistent monitoring.

Security event overload and **security analyst burnout** are also systematic problems for IT teams that have to deal with all security operations in addition to their regular workload. Seventy-one percent of SOC analysts say information overload makes their jobs stressful (Ponemon). Because the number of logged events can quickly climb into the millions over the course of a day, modern security concerns will quickly overcome a SOC-less organization.

Although some organizations may feel that more security analysts will serve the same purpose as implementing a SOC, hiring too many analysts leaves a company in a situation where they are **spending too much to achieve lackluster results.**

How a SOC Can Overcome These Challenges

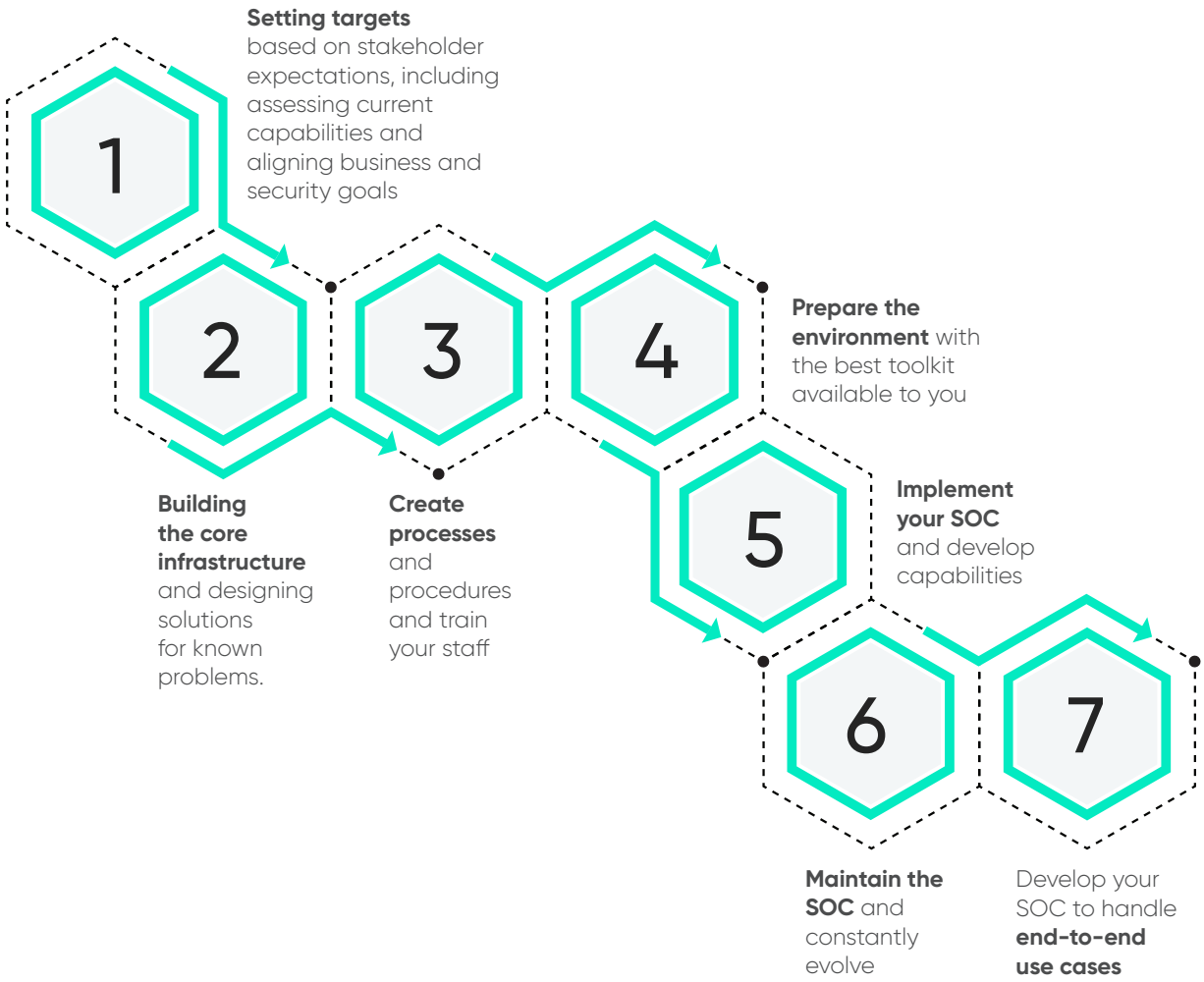
As well as dealing with ineffective hiring practices, security burnout and overload, and reducing the amount of time that passes between an incident and its discovery, a SOC also provides a company with these benefits:

- **Increased data security** through better responses to security issues
- **Improved analytics,** including network traffic and threat intelligence
- **Better workflows for security teams,** leading to better incident response protocols and less employee burnout
- **Machine-assisted threat hunting,** improving your ability to find hidden threats within your own systems
- Better incident response through **risk-based threat triage,** meaning less time is wasted and fewer known threats slip through the cracks
- A more **secure platform** that incorporates a variety of tools and systems to support effective security practices

As your SOC matures, each of these key factors must be improved. Using new tools, adding specialized security professionals, and developing your playbooks is necessary for the ongoing success of a SOC.

How to Set Up a SOC in Your Organization

SOCs do not need to be ready to battle with a state actor overnight. Instead, you should work towards building secure foundations and maturing the system as your security needs and capabilities expand. For an organization beginning to build a SOC for the first time, establishing a SOC has seven key stages:



When you have established this key functionality, you are ready to let your SOC mature through specialized personnel and business-specific tooling. But how do you effectively implement these changes?

The Key Stages to Establishing Your SOC

Setting up a successful SOC for the first time can be achieved with these seven steps. Understanding your organization's threat model and the necessary tools to handle your adversaries is key to building a SOC solution that stands up to the threat of the modern threat landscape.

STAGE 1:
SETTINGS TARGETS: WHAT SHOULD A SOC DO?

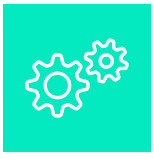
Before an organization can create a security operations center, the responsible security team needs to identify the overall goals of the SOC, how they will integrate with business goals, and the core functionality that is necessary to begin security operations.

ALIGN BUSINESS AND SECURITY GOALS

Security measures are worthless if they do not cater to the needs of the business. All aspects of business and security must be aligned to identify what aspects of a SOC are important to establish first.

ASSESS CURRENT CAPABILITIES

Most large organizations now have at least a small security team handling threat intelligence, intrusion detection, incident response, and recovery. With the basic tenets of a security team in place already, making the jump to a full SOC will be easier. If not, you may need to recalibrate your expectations of how quickly you can build.



STAGE 2:
IMPLEMENTING CORE FUNCTIONALITY

When building up a SOC, you don't need a war room from day one. Cover the most basic needs of your organization and cover them well. Establishing the basics correctly at the beginning creates a strong foundation for your SOC to mature upon.

Although each organization has different needs, these four factors help create a strong basis:

1. **A SECURITY MONITORING SYSTEM**
   A necessary stage in understanding all incoming threats
2. **AN INTRUSION DETECTION TOOL**
   To identify and find the adversary as they try to circumvent your defenses
3. **AN INCIDENT RESPONSE PLAN**
   Including playbooks for known threats
4. **DATA RECOVERY PROTOCOLS**
   Including disaster planning such as ransomware lockup or total destruction of the SOC headquarters

After that baseline has been established, the SOC and all security operations center roles can begin to mature.

STAGE 3:
DESIGNING THE SOC SOLUTION

Because business goals and security goals are now aligned and the basics have been established, the SOC team can now focus on developing threat intelligence and security operations.

IDENTIFY BUSINESS SPECIFIC NEEDS

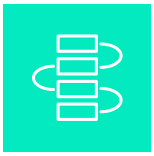
Using your collected data, your SOC team should identify key security concerns that the organization faces. For example, if there is a proportionally large number of phishing attacks, resources and training should be given to mitigating the success and severity of phishing.

DEFINE NECESSARY STEPS

Business-critical use cases can be established in the form of playbooks. This will then help security analysts to handle the most common issues the business faces and improve incident response.

CREATE ROOM FOR FUTURE USE CASES

As your organization changes, your security posture will need to change too. Creating processes that allow you to easily spin up new use cases will reduce the amount of time spent on expanding your security operations and improving your ability to respond to security risks.



STAGE 4:
CREATE PROCESSES, PROCEDURES, AND TRAINING

Closely tied with identifying and defining business needs, full-scale processes, procedures, and training needs to be rolled out to answer the problems that were previously defined.

IDENTIFY BUSINESS SPECIFIC NEEDS

Event logging can tell us practically anything we want to find out about the endpoints we work with, but understanding what your organization needs to log is key to successfully implementing processes, procedures, and training. Understand your organization's needs and you will be able to monitor what is necessary and ignore what isn't.

DOCUMENT PLAYBOOKS

Where procedures have matured, the SOC creates playbooks to deal with known, common threats. Creating playbooks (i.e. a plan that details the appropriate response in the face of a cybersecurity event, including a plan for all security roles) for known entities streamlines the time that is spent on each issue by your SOC analysts.

EMBRACE AUTOMATION

Automated responses are key to reducing the workload on your security analysts. Security analysts face burnout when they have to deal with the same repetitive tasks every day. Why not turn to automation in order to handle your log management or responses to known minor threats?

Implementing automation and orchestration will allow your security teams more time to spend on developing and strengthening your security posture instead of burning out and potentially missing a serious threat.

TRAINING FOR EVERYONE

Everyone is in this together. In the past, many organizations have treated security operations as a distinct and almost alien part of the organization. Integrating security into every department and providing training to help reduce the overall risk of the adversary gaining access to your systems.

STAGE 5:
PREPARE YOUR ENVIRONMENT WITH THE BEST TOOLS AVAILABLE

A SOC is only as effective as the tools it uses. Whether you use commercial tools, add open-source toolkits, or build your own on-site, your SOC must implement a toolkit that is specific to your organization's needs.

This stage is organization-specific and your security team can only build their environment when they truly understand the needs.

ASSEMBLING THE TOOLKIT

For small organizations, using a variety of open-source tools is a perfect way to address known issues that are specific to your organization. While third-party commercial tooling might be more effective in the long run as your organization grows, understanding your security needs helps you create useful security strategies that are business-specific.

STAGE 6:
IMPLEMENTATION

For many SOCs, the implementation stage is the one that brings the most issues. Making the jump from a security-conscious IT team department to a full SOC requires a refinement of skills, tools, and techniques that need to be brought to maturity as quickly as possible.

BUILDING AN INFRASTRUCTURE FOR MANAGING LOGS

Log management quickly turns into data-based madness when it is not approached carefully. Your logs should be collected, organized, analyzed, compressed, and then stored securely for compliance monitoring or even potentially finding the tell-tale signs of a breach that had evaded normal security protocols.

DEVELOPING ANALYTICS CAPABILITIES

Your future security posture relies on your ability to gather analytics and change your security posture based on the findings. Using endpoint data gathered prior to making changes, developed analytics capabilities will help turn a SOC into a responsive security center that is constantly improving the way in which it detects, intercepts, and analyzes threats as the adversary launches them.

MORE AUTOMATION, MORE ORCHESTRATION

In an effort to stop your SOC personnel from burning out, your team should constantly be automating the known issues and orchestrating the automated responses to create fully-automated workflows.

DEPLOY END-TO-END USE CASES

Your use cases need to be developed into full playbooks that deal with security threats as soon as possible. From detection to remediation, your team's approach should carry every potential incident through to full operations with data-informed security development and consistent use case testing.

REACT TO THE DATA

Log data is a powerful tool for SOC teams that have the correct analytic skills and create new policies based on what they have observed. Take the data and create new processes or playbooks that cut down on time spent dealing with security issues and threat actors.

TEST YOUR HYPOTHESES

After creating a hypothesis based on the recorded data, test your solutions. SOC analysts can act as a red team, pentesting the system and pushing intrusion detection systems in order to fully understand your organization's security posture.

Consistent testing will help your SOC team understand the weaknesses in the system and help them improve the SOC's overall capabilities.

PROVE RELIABILITY

When your team can react to new threats and test their own capabilities, you will develop a reliable system that is provably sturdy against the ever-expanding threat landscape that companies face today.

STAGE 7:
MAINTAIN AND EVOLVE

Although this is the final stage of establishing your SOC, it is only the beginning of building effective defenses. In order to improve your security posture with your SOC, there are three key areas your team must focus on:

1. ALWAYS FINE-TUNE YOUR SOC

Just because a playbook or rule works now, does not mean that it will work in the future. Tuning your approach to account for changes in known threats or more efficient ways of dealing with them will help your SOC team stay on top of the threat challenges your organization faces.

2. CREATE REVIEW PROTOCOLS

Just like you have developed playbooks for dealing with security issues, you should create protocols to streamline your review process. In this way, your SOC personnel will evolve your system with the same level of structure that they approach intercepting and managing new threats.

Similarly, reviews do not stop at the response protocols you use. Examining and improving your staff and models is key to better security protocols and expanding your capabilities when the opportunity arises.

3. INTEGRATE OTHER SYSTEMS

As you begin to use new systems to support your security team, your SOC can mature and start gathering information to improve your analytics and better inform your security response.

Your SOC personnel should be able to integrate data that is collected from a SIEM, firewalls, anti-virus/anti-malware software, and use all relevant information to empower your analysis and ability to respond to a security incident.

DIY SOC vs. "Plug-and-play" SOC Solution

After these stages, your SOC team should now have all the tools, playbooks, and processes to successfully manage the security of your organization. This also allows space for further development and for your security team to bring the security operations center to full maturity.

Finding the best SOC personnel and improving or adapting your security systems is a slow process. Many organizations will need time to tie all business goals to security, but everyone has their part to play when investing in a SOC. Defending your critical infrastructure and developing advanced security measures is the natural next step to following our guide on setting up your SOC.

Building a SOC isn't an easy task. For companies that cut corners, the effectiveness and cost of a poorly constructed SOC will quickly become a drain on business resources without having much to show for it. Secure foundations lead to mature SOCs and weaknesses in your foundations will compromise your organization's security posture.

That's why many organizations are now turning to third-party security experts to set up, maintain, and sometimes remotely manage SOC capabilities for their organizations.

Alternative to Building an In-House SOC: A SOC Infrastructure Solution

Acquiring all the tools for a full SOC internally takes time, but using external SOC infrastructure will bring your security response up to standard and beyond very quickly.

That's why turning to solutions such as CYREBRO's SOC Platform enables businesses to reach a high-level security posture through advanced detection algorithms that monitor, analyze, and interpret incoming events.

An interactive, cloud-based SOC platform like CYREBRO gives users instant visibility into their security posture without the need to acquire technology and personnel and build a SOC from the ground up. SOC platforms are used by businesses of all sizes, with SMBs benefitting from enterprise-level security solutions and expertise. It is technology agnostic, meaning it integrates seamlessly with whatever tools or systems your organization is using. The platform is backed by the capabilities that are required for a complete SOC: strategic monitoring, incident response, threat intelligence, SIEM optimization, threat hunting, and digital forensic investigation.

Want to learn more about how you can leverage SOC infrastructure to improve your existing solutions, without the need to build a SOC in-house? Learn more about CYREBRO's SOC capabilities, or schedule a demo to see it for yourself.

Learn more about CYREBRO