laya tech™

How to Build a Security Operations Center (SOC) within a budget?

In this era of technology, unfortunately, cyberattacks are becoming the norm. Keeping up with the increasing rate of cybersecurity vulnerabilities may seem near to impossible when your enterprise is lacking in-house security resources as well as professionals- that's why building a Security Operation Centre (SOC) is an ideal solution.

While maximum organizations understand the significance of SOC, several organizations report that they are not able to afford a 24x7 in-house SOC. That's why Laya tech comes with an ultimate solution to building a SOC within a budget. Let's find out how it can be possible.

Before going into the details of building SOC, let's have an idea of what does a SOC means.

If your company is functioning without a SOC, then you could be at high risk for critical delays in finding out and responding to those incidents. Anomalous activities or threatening could go unnoticed and your business may be at a greater risk of becoming a victim of a cyberattack. Another heavy cost of not having a SOC includes:

>> Your enterprise can't be monitored continuously 24x7.
>> There are important delays in responding to several events.
>> Potentially damaging security activities may go unmonitored.
>> Job satisfaction is low because of the heavy workload and immense manual work.

Have you faced any of these issues? While these are normal challenges, the issues are not sustainable. For enterprises caught between the excessive designing cost of formal SOC and completely insufficient protection from an informal SOC, there is a solution: Build a SOC that automates as much work as possible so that your professionals can concentrate on other important works.

Security Operation Centre

Prevention	Detection	Response
Data Protection	Log Management	Incident Response Plan
Network Security	SIEM	Breach Preparation
Application Security	Threat Hunting	Table Top Exercise
End Point Security	PT | Red Team	Forensics
Security Configuration	Web App Scanning	Breach Communication
Zero Trust	Vulnerability Scanning	
Patch & Image Management	DLP | UBA	
NOC	Threat Intelligence	
Cyber AI	Big Bounties	

Key ingredients to build a SOC

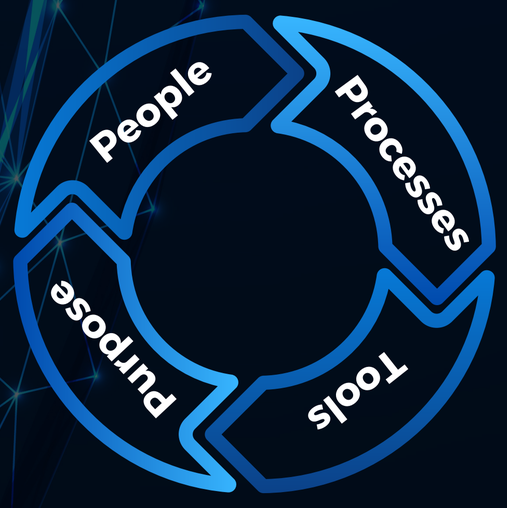
Security Operation Center (SOC) is responsible to detect, monitor, contain and remediate IT vulnerabilities across vital applications, systems, and devices in their public as well as private cloud environments. Utilizing several processes, and technologies, SOC teams depend on the current threat intelligence to decide whether an active threat is occurring, its impact, and the proper remediation. All the key elements to building a SOC include:

People:

The team of Security Operations Center (SOC): Review the roles and responsibilities of security operations to build a SOC team. Evaluate their skill set matrix to help with recruiting a strong SOC team.

Processes:

Establish the important processes you will require for building a SOC. These include prioritization and analysis; categorization and triage; remediation and improvement; and audit and assessment. Laya Tech helps you to centralize these processes and implement them carefully.



Tools:

Review all the required security monitoring tools you will need to build a SOC including vulnerability assessment, asset detection, intrusion discovery, behavioral scrutinizing, and SIEM/security analytics. You can explore the real-world advantages of consolidating these required tools in Laya Tech.

Purpose:

Understanding the actual purpose of establishing a SOC is very important. Identify the differences among strategic, tactical, and operational intelligence and the particular ways that are utilized within the SOC.

How do I know whether I need an MSSP or not?

Next, you should know when you want to outsource your SOC to a potential service provider. Staff size and their skill sets are important factors. At the same time, several big enterprises depend on MSSP (Managed Security Service Provider) rather than building their SOCs. The preference truly comes down to answer one question: Whether you can give the guarantee that your team has all the required resources as well as skilled professionals to identify, contain, and respond to a data threatening? If your team is focused on other existing sectors, it may be useful to use an MSSP to manage your SOC.

SOC - An Enterprise Suite

Features & Outcomes of SOC

> 24/7/365 security governance on People | Process & Technology
> Scalability & Flexibility
> Ongoing Business Focus
> Lower Personnel cost
> Long-Term ROI
> Continuous Protection & Compliance
> Improved Business Reputation
> Cyber Excellence
> Quick & Effective Response
> Operational ease and secured way of Backup|Storage & Recover

Using a variety of technologies and processes, Laya's SOC teams rely on the latest threat intelligence to determine whether an active threat is occurring, the scope of the impact, and the appropriate remediation also offers:

- Security status of your IT infrastructure and Critical Assets
- Prioritize Alarms & Vulnerabilities
- Prevention, Detection & Response
- Visibility Score Card

With growing customer expectations in ever-changing business arena, Laya offers world-class tech and talent aims to deliver a tangible business outcome for our clients thereby creating a niche value preposition.

We are at your service and please let us know, when we shall schedule a demo to help you to understand the features, Services & benefits of availing the services of Laya's SOC Team as part of long-term ROI and cyber excellence.