MSP1

SOC: Build or Outsource

Most CIOs face this question for most of their IT decisions. However, the decision to opt for any of the SOC models; in-house, outsourced (as a Service) or hybrid, is a tough one.

Inhouse SOC

An in-house SOC model is usually adopted by organizations that have compliance issues with respect to outsourcing or see outsourcing as a perceived risk that could affect the integrity and functioning of their business.

The downside to this approach is that the upfront expenditure of building a SOC in-house is considerably high as compared to an outsourced or shared one. It will take years for an organization to realize the RoI on the CapEx with respect to licensing of SIEM tool, threat intelligence and setting up the infrastructure.

Moreover, finding experienced SOC analysts or managers to man the SOC will be difficult as these professionals are not easy to find. Security is a domain where constant knowledge sharing is one of the key levers to successfully prevent attacks. A captive SOC performs like an island in itself. Even if the organization has been able to deploy the best of people and technologies, the inability to connect with a larger ecosystem can lead to a serious knowledge gap.

There are other factors as well to consider when building your own SOC. It becomes an exercise in bringing together the right tools, intelligence and people together to create an integrated solution

Outsourced SOC

In an outsourced SOC model, the service provider provides the infrastructure, intelligence and other capabilities. An experienced service provider has a state-of-the-art security infrastructure and core competency that provides rich threat intelligence to detect real time sophisticated and targeted attacks. They already have a team of trained and experienced security analysts well conversant with most of the security threats that an organization may face. And, by the virtue of their engagements with multiple clients, they are equipped with state-of-the-art tools, as well as, a sound knowledge about possible security threats and incidents (both current and evolving). Hence, the costs are lower than an in-house solution.

The hybrid SOC

This model allows an organization to leverage its own strengths and resources, while being supported by cybersecurity experts with advanced expertise and tools. Some organizations choose to supplement their in-house SOC with
an outsourced second SOC, while others want to simply augment their internal resources while they work on getting their internal SOC off the ground.
Either way, having a second set of eyes on the network at all times gives you a higher level of protection and confidence knowing that your valuable information is safe.

"We consider the MSP1 SOC an extension of our team. When we have questions around any alerts we receive, we feel confident that within minutes of reaching out to MSP1 we will get a response explaining actions we need to take."
-Garret Firstbrook, CIO

Contact Sales

+1 (408) 769 5030

+91 9769757668

www.MSP1services.com
info@msp1services.com

MSP1 helps businesses fight cybercrime, protect data and reduce security risk. We are a leading provider of cybersecurity solutions and services. Through our global SOC and delivery center we monitor detect, contain and remediate IT threats.

With integrated technologies and our team of security experts we enable businesses to transform the way they manage their information security and compliance programs. Our services are customized, tailored and white labeled that fit your budget.