Six Benefits of Outsourcing your Security Operations Center

Security Operations Centers (SOC) are facilities that house cybersecurity teams who monitor, detect, and respond to threats providing a critical element of all good I.T. security programs. Here I make an argument why outsourcing to a managed 24/7 SOC can often be more effective than having an in-house team.

It enables immediate access to talented, certified cyber professionals around the clock, shared threat intelligence, segregation of duties, scalability, reduced barriers to entry, and lower ongoing costs.

SOCs are generally vastly different from an organization's critical operations, therefore it makes sense to leave it to those who consider it their core business.

1. Finding and maintaining a talented SOC team is expensive

Deploying a SOC locally requires hiring new employees who are 100% conversant with the security industry and experienced with Security Information and Event Management (SIEM) tools. Unfortunately, finding talented people to address all SOC related issues can be difficult and time-consuming. Cyber attacks don't just happen during business hours. 24/7 monitoring guarantees the quickest response time to identify and remediate potential threats, however the added complexity of shift rotation related to around the clock resourcing creates

An outsourced SOC enables immediate access to talented, certified cyber professionals around the clock, shared threat intelligence, segregation of duties, scalability, reduced barriers to entry and lower ongoing costs.

an additional burden on HR, facilities and management. Even if successful in hiring security experts, it may be difficult to justify keeping them in-house due to the high costs of their salaries. Although security attentive, most organizations have a limited budget and outsourcing the SOC and SIEM is a good middle ground.

2. Outsourcing provides segregation of duties and lowers conflict of interest between departments

Organizations know the expectations and implications of outsourced SIEM and SOC beforehand, including service requirements and budgeting. Contrary to this, locally deployed SIEM undergo a "learning curve." As new security teams master the industry, their needs can encroach on other departments. A good example is when the security team insists on purchasing high ticket items when the company is strapped for cash. Of course, this will raise eyebrows, yet failing to comply with the team's requirements may lead to an incomplete and compromised SOC.

Not only does outsourcing reduce the time to become operational it also reduces the cost of implementation and ongoing management.

3. Long-term return on Investment

Outsourced managed security providers that have focused on mastering the security industry with specific focus on SOC and SIEM are highly effective and productive in their space. They have regular experience implementing SIEM tools and have greater access to specialized talent. Not only does outsourcing reduce the time to become operational it also reduces the cost of implementation and ongoing management. This provides a good long-term return on investment getting everything at a fraction of the cost if completed internally.

4. Benefit of trends and detection on other customers

Outsourced SOC takes advantage of optimized services based on trends and the detection of other customers. Designing an in-house SOC requires time and investment, and ultimately is likely to fall short of an optimized, integrated solution. Since a local security center relies on a limited set of data, there are many benefits from the best practice an outsourced SOC provides.

5. Enhancing efficiency in order to concentrate on core operations

Have you ever asked whether you are getting enough time to concentrate on your core operations? Due to their nature, SOCs are generally vastly different from most organizations' core focus. They require a secure environment, highly capability IT security personnel working around the clock with specific toolsets. Outsourcing enables management to get back to what matters in their organization.

With a quick and effective response time to cyber threats, it can save a company millions of dollars from legal costs, reputational damage, customer churn and business disruption.

6. Scalability and flexibility

All business needs are not the same. For instance, a start-up company may require only a single security expert working for a few hours a day. When the service is outsourced, the needs are pooled with those of others to hire a full-time team. The team is also effective through collaboration and developing solutions together to react quickly. There is the benefit of access to additional resources. This can range from immediately in the event of a severe incident or the more gradual growth of a business and consequential data to protect. With a quick and effective response time to cyber threats, it can save a company millions of dollars from legal costs, reputational damage, customer churn, and business disruption.

Simply Secure Group is run by a team with a wealth of experience delivering cybersecurity solutions and specializes in running an Outsourced Security Operations Centre for their clients in line with the above article.

If you'd like to know more, please feel free to reach out to me personally on +1-954-684-5850