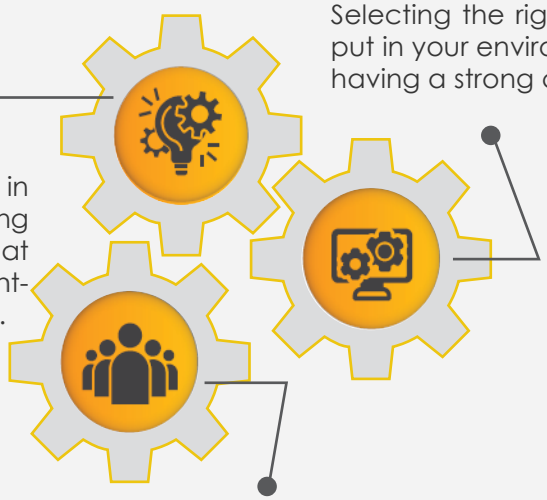
inspira®

Innovation I Impact I Integrity

Finding the perfect balance for your Security Operations Architecture

Organizations today are aware of their cybersecurity risk, but many struggles to determine what is the best way to stay protected. Finding the right balance between using internal resources and outsourced managed services is the key to a successful cybersecurity program. But how does an organisation evaluate their need to control technology and operations with the size and skills of the existing in-house cybersecurity staff?

The three fundamental pillars of a strong cyber defence program are the people, process, and technology:



Technology
Selecting the right technology mix to put in your environment is essential for having a strong cybersecurity posture

Process
Having good processes in place keeps the team running smoothly and ensures that security events are documented and handled consistently.

People
Security teams must have the skills to manage your devices and monitor security alerts, but also to build the appropriate content to detect threats quickly and accurately within your environment.

Allocating resources to each of these elements and defining how they work together can be a challenge – one that can take several iterations before getting it right. More and more organizations are moving towards Hybrid SOC models where security operations are shared by in-house staff and an outsourced partner.

To determine the right model for your organisation, consider the following:

Who owns the SIEM?

For some enterprises, purchasing and maintaining a SIEM is the ideal option. It gives them full ownership of both the technology and content and allows them to build a security infrastructure that meets their specific needs.

But purchasing a SIEM is expensive and comes with its own set of challenges.

When looking at this option, one must consider things like:

- Who is going to install the SIEM? Where will it be deployed?
- Who will create the searches and analytics you use to discover threats? Will they be regularly updated and tuned for your environment?
- How much time will your team spend managing the system?
- Who will monitor security events?
- How do you integrate and curate threat intelligence into your analytics?
- How do you increase capacity as your organization grows?
- Do you need a redundant architecture?

Staffing is often the biggest challenge as many organizations struggle to recruit and retain qualified individuals to manage and monitor their SIEM. An organisation needs to ensure that have 24/7 coverage, including staff committed to working the graveyard shift to avoid coverage gaps, and building a Cyber Security Operations Centre (C-SOC), that will need multiple skill sets including SIEM content developers, Security Engineers, Threat Hunters and Incident Responders. Organizations that do not have the ability to support specialization often look for outsourcing some or all of their security operations.

Fully Managed Model

If owning the SIEM is not a viable option for your organization, you may consider fully outsourcing your security operations. Under this approach, a Managed Security Service Provider (MSSP) sends security events from multiple clients to a centrally hosted SIEM. The MSSP takes responsibility for detecting indicators of attack or compromise and alerting their clients accordingly.
Using a fully managed service is attractive to some organizations because it does not require users to buy complex software or staff a C-SOC. Moreover, MSSP clients benefit from an OPEX model, reduced cost of ownership reduced cost of ownership, and a service that can scale to meet the needs of a growing business.

Hybrid Model

Organisations try to manage their on-premise SIEM but find it difficult and complex due to lack of processes and skilled manpower. Some try engaging a fully managed SIEM but realise that they need more control over their technology stack and data.

Ideally partnering with an MSSP to create a hybrid model allows an organisation to own the technology components but outsource the 24/7 monitoring and management, reducing staffing challenges and lowering the OPEX. A good MSSP will create a personalized runbook, set up business context modelling to understand the high-value assets, and provide the metrics, so that the present security posture can be presented to the board. The MSSP will have the expertise to properly configure the SIEM – from data ingestion to use cases – and will be available to tune it over time to keep it running optimally. In addition, components for automation, orchestration and threat intelligence can be added to increase the maturity of the C-SOC.

Selecting the right MSSP is critical, as they are an extension of an organisation's security team. Since most organizations cannot staff a 24/7 SOC, their in-house team should not feel threatened by the possibility of job loss; rather, they should embrace the opportunity to focus on more varied and challenging tasks.

What's Next?

The threat landscape continues to evolve. Attackers will only get smarter, faster, and more creative, so organizations need to stay ahead of tomorrow's cyberthreats. Whatever approach is chosen, make sure you have got a partner with experience and a vision for the future.

Inspira Enterprise is an industry leading Managed Security Service Provider (MSSP), utilizing next-generation technology and methods to detect advanced threats and automate responses. Contact Inspira to learn about our customized security options and see how we can help your company stay protected.

inspira®

Innovation I Impact I Integrity

+91 9920335957 | +91 22 40569999

info@inspiraenterprise.com | inspiraenterprise.com

Follow Us

BLOG