inspira®

Innovation I Impact I Integrity

Why Switch to a Hybrid SOC?

In today's heightened threat environment, cybersecurity leaders must find creative ways to leverage their resources and better defend against advanced cyber attacks. Balancing the cost of cybersecurity operations vs. the risk of a security breach is one of the toughest challenges facing cybersecurity leadership. CIOs and CISOs are seldom thanked when nothing bad happens and, despite making their best efforts within a limited budget, usually blamed when a security incident does occur.

Hybrid SOC

Enterprises can generate hundreds of millions of security events every day & these events must be collected and analyzed around-the-clock to detect actual or pending attacks. Conventionally, organizations have staffed Security Operations Centers (SOCs) and deployed SIEM technology as the corner stone of their security event monitoring programs.

However, today many forward thinking enterprises are adopting hybrid models where some or all of these functions are outsourced to service providers.

The Challenges of Building and Operating a SOC

People

- Shortage of qualified professionals
- Delays in hiring SIEM experts
- Employee training and retention

Process

- Achieving visibility to new threats
- Maximising effectiveness of investigations
- Cost and time to operationalise SOC

Technology

- SIEM configuration and tuning
- SIEM use case development and customisation
- Resilience of platforms and connectors

Economics

- CAPEX to build and scale systems
- High salaries and expensive consultants
- Cost and complexity of 24x7x365 operations

Why Outsource Security Event Monitoring

1. Challenges in Hiring and Retaining Security Specialists

With an unprecedented shortage of qualified cybersecurity professionals, organizations face the most challenging job market in history. Many organizations find it difficult to attract and retain qualified security experts causing gaps in the efficacy of their security operations. Experts in SIEM technology are particularly expensive to hire and retain. SIEM consultants can backfill gaps in hiring, but they command a very high hourly rate.

Managed Security Service Providers (MSSPs) are attractive employers because they offer competitive salaries, opportunities for skill enhancement, and security focused career paths.

2. Threat Visibility

Cyberattacks are constantly morphing as hackers exploit new vulnerabilities and create new variations of malware. CryptoLocker, CryptoWall, and other variants of ransomware are prime examples of this. Service providers are often the first to see new attack vectors and techniques as their customer base encompasses organizations in many different industries and locations. Compared to individual enterprises, users of a managed security service may also benefit from more sources of third party threat intelligence feeds and advanced correlation analysis between threat intelligence data and other suspicious behavior. Overall, improved threat visibility increases the chance of detecting and preventing a cyber breach.

3. 24 x 7 Vigilance

Advanced cyber attacks frequently originate from Western Asia, Eastern Europe, China and other countries that function outside normal business hours. Just blocking traffic to or from a country like Russia or any country does not address this issue because hackers have antici-

pated this countermeasure and now launch their attacks from IP addresses in countries perceived to be lower risk.

Effective security requires around-the-clock monitoring to detect and respond to targeted attacks before they result in loss of data and damage to an organization's brand. Often staffing and managing a 24×7 SOC is beyond the resources of an organization, but service providers can provide this capability to their customers at a reasonable cost.

4. Lack of SIEM Content

The underlying effectiveness of a SIEM system is driven by the rules and use cases that detect indicators of attack, indicators of compromise, or policy violations. Depending on the size and complexity of an organization's infrastructure, a fully functioning SIEM may have hundreds of use cases. Default use cases provided by SIEM vendors are ineffective and not mapped to the specific technologies and applications used by a SIEM user.

Building SIEM content is time consuming and requires an in-depth understanding of the threat landscape and the logic by which security events are mapped to different attack vectors and vulnerabilities. Well-tuned rules and content help increase the productivity of Security Analysts' investigations ensuring their time is spent on the most critical events and not chasing false positives.

Service providers can leverage the cost of developing SIEM content across many customers and dedicate resources to continuously develop new and customized rules and use cases.

5. More Effective SOC Analyst Investigations

No SIEM can provide 100% accurate alerts. Security experts are needed to investigate suspicious alerts to determine the criticality of a threat. In a high performance SOC with a well-tuned SIEM, you can expect the following:

- Half of all high priority actionable alerts are the result of Security Analyst investigations
- Of all the system alerts requiring analyst action, after investigation, about half turn out to be false positives

These data points underscore the importance of having sufficient human security experts available 24×7.

Service providers augment the existing team of Security Analysts and can often more effectively filter and correlate security events to present Security Analysts with better data. Outsourcing monitoring tasks also improves the morale of existing employees and allows them to focus on other priorities.

6. Rapid Response

Responding rapidly to security incidents is as important as the ability to detect and prioritize security threats. Critical events require response by senior security analysts and, if needed, remediation actions like wiping a laptop, blocking an IP address, or quarantining a file.

Effective incident response requires security experts to be available on a 24×7 basis, which is not always possible for even large organizations with dedicated CSIRT teams.

Next-generation SOCs are increasingly automating responses to critical security threats. For example, automating blocking an IP address on a firewall after detecting network reconnaissance from a known malicious IP address targeting a high value asset. Temporarily blacklisting an IP address provides IT teams time to investigate the threat and remediate it if necessary. At companies where operations teams are not available outside standard business hours, this approach is particularly useful. Building automated response actions requires fine-tuned use cases along with integration and testing resources.

7. Operational Excellence

It is a truism that maintaining effective security operations requires combining the use of people, process, and technology. Managing these elements is non-trivial. The Target stores data breach exemplifies this point as their SOCs in Bangalore and Minneapolis reportedly received priority malware alerts, but failed to act on them.

Maybe their Security Analysts were swamped with other alerts. Perhaps their runbook, which should have described detailed processes and escalation procedures, was not clear or updated. Service providers that have sophisticated support systems, trained personnel, and fine-tuned procedures and workflow can help their customers achieve operational excellence.

8. Time and Money

The decision to outsource security event monitoring is heavily influenced by the risk of operating at a diminished level of security effectiveness. Building a SOC and tuning a SIEM takes from months, sometimes years, with a long list of dependencies including hiring, training, and system integration efforts. Service providers reduce their customers' exposure to security breaches during periods where security operations are not operating at full speed.

Service providers also have greater potential to leverage economies of scale than single business entities. This is particularly true in a 24×7 operation where of the 1095 eight-hour shifts in a year, only 260 are during normal business hours.

Inspira is a leading Cyber Security Operations Centre (C-SOC) Transformation service provider. We combine state-of-the-art analytics with around-the-clock security monitoring to provide advanced threat detection and breach prevention solutions to financial services, enterprises, healthcare providers, and government.

inspira®

Innovation I Impact I Integrity

+91 9920335957 | +91 22 40569999

info@inspiraenterprise.com | inspiraenterprise.com

Follow Us

BLOG