RocketCyber
A Kaseya COMPANY

THE ADVANTAGES OF A SOC

Security operations centres run 24x7x365. This uninterrupted monitoring is critical to detecting the first signs of anomalous activity. Attacks don't only occur Monday through Friday, 9 to 5. Without SOC services, cyber-criminal attacks can remain hidden for a long time as companies do not have skills to detect and respond to threats in a timely manner. When we look at the average attack dwell time, 43 days on average for ransomware versus months or even years for more persistent threats (200 days). SOC's shorten the dwell time from months down to minutes, reducing the financial impact when an intrusion does occur.

SOC will allow MSP's to have a better visibility into their customers environment, have skills, processes and continuous improvement. With more and more regular attacks, many MSP's are refocusing their security efforts on prevention, detection and response.

Decreased costs of breaches and operations:

- By minimising the amount of time, a cyber attacker lurks in a customer's network, the SOC team can reduce the effect of a breach and, therefore, the potential costs the breach may incur via data loss, lawsuits or business reputation damage. The longer an attacker remains in a system, the more potential damage can be done to the company.
- Finding skilled candidates and hiring internally for most cyber related positions is a difficult task due mostly in part to the lack of security professional available for hire.

Threat prevention:

- SOC's are about more than just detecting incidents. The analysis and threat hunting conducted by SOC teams help prevent attacks from occurring in the first place. SOC's provide increased visibility and control over security systems, enabling the MSP's to stay ahead of potential attackers and issues.
- SOC monitoring around the clock keeps the threat radar circulating, hunting out advanced TTPs (tactic, techniques & procedures) to malicious hosts, networks and cloud artifacts, before a breach occurs.

Improved threat management

- MSP's regularly deploy a variety of security technologies designed to prevent and detect threats, as well as to strengthen and protect assets. For maximum efficiency, they must be centralised, standardised, correlated and monitored in real time, with resources available to analyse and respond to suspicious activities and incidents.
- Consolidating security functions in a SOC can save money.
- Incidents are often likely to span multiple entities, and this requires coordinated actions to reduce risk. A SOC perfectly meets all these requirements.
- With SOC, MSP's will have greater speed in identifying attacks and remedying them before it causes more damages.

Maintenance of regulatory compliance:

- A SOC also helps you to meet regulation requirements that require security monitoring, vulnerability management and incident response function.
- SOC 2, HIPAA and GDPR.

SOC as a Service:

- To protect themselves and their customers from today's cyber threats, most MSP's (MSSP's) set up a Security Operations Centre (SOC) with trained staff and costly technology (SIEM), as well as all the constant training and maintenance that go with it.
- SOC is often not an option because of its constraints and costs of implementation. Using an external third party SOC like RocketCyber is a reliable and efficient solution with a reasonable cost while benefiting from a high-level expertise and skills.

To summarise, having a SOC allows you to have dynamic security that acts as a real bastion of analysis, monitoring, prevention and remediation

- The drive towards digital transformation and cloud services to improve efficiencies, increase agility and cut costs has rapidly and vastly expanded the attack surface of most organizations.
- Best-in-class incident response without long deployment periods, faster detection and remediation of threats, improved security visibility and reporting through 24x7x365 monitoring, with predictability affordable costs.
- Consolidate all security threats, tools and systems into a single dashboard to address and resolve all alerts at a fixed and predictable monthly or annual cost.
- Resolution of all alerts to get maximum value out of existing systems.
- Improved incident response times and practices.
- Faster detection of security events such as compromises and containment of threats.
- Reduced cost and business impact of security incidents.
  And much more

RocketCyber
A Kaseya COMPANY