The Benefits and Barriers of Having a SOC

CYBER THREATS – A TRUE CONCERN FOR ANY ORGANIZATION

It's no longer a secret that any firm, regardless of size, is at risk for cyberattacks. In fact, SMBs experienced a 424% increase in cyberattacks since 2020 and the average cost of cyberattacks to a small U.S. business is $25,612. With 60% of SMBs not recovering from cyberattacks and going out of business within 6 months, this risk keeps SMB executives up at night.

Why are SMBs being targeted by cybercriminals? Unlike larger organizations with ample funds to build their cybersecurity practice, traditionally SMBs didn't invest much in their cybersecurity. Smaller businesses just didn't have the resources – money, people and expertise – to build a comprehensive security practice. That led to SMBs becoming more vulnerable. And as such - they are easy targets.

Cyber threats are constantly becoming more sophisticated and simple security solutions that typically serve SMBs are no longer sufficient. While large organizations can fight against advanced attacks by leveraging a Security Operations Center (SOC), SMBs can't afford that either and stay behind, becoming even better targets for bad actors.

How can small businesses achieve enterprise-levels of security without making unreasonable resource investments? **Managed SOC may be the answer.**

WHAT IS MANAGED SOC?

A SOC, or Security Operation Center, is a command center made up of highly skilled security personnel, processes and cybersecurity technologies that continuously monitors for malicious activity while preventing, detecting and responding to cyber incidents.

A managed SOC is an outsourced service that provides managed detection and response (MDR). This continuous monitoring protects organizations, searching for threats aiming to penetrate the organization and mitigating them as soon as they are found.

WHY SOC?

Considering the constantly growing risk of cyber-attacks on businesses of all sizes, nowadays even the smallest organizations need to have continuous, 24/7 monitoring and response service available to them.

Plus, with small business IT departments stretched thin and having to tackle not only cybersecurity, but all other aspects of technology operations, turning to an external resource enables IT leaders to efficiently focus on the projects and activities that matter most.

The Benefits and Barriers of Having a SOC

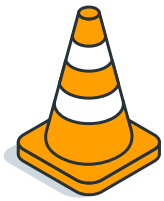
THE BENEFITS

Utilizing a managed SOC gives small business IT departments an effortless solution to gain 24/7 managed detection and response and advanced threat protection from ransomware, credential harvesting and other cyber risks that can cost businesses thousands.

A managed SOC also increases an organizations' defense-in-depth posture by providing real time threat detection and response, helping businesses mitigate cyber threats as they occur. This dramatically reduces risk exposure and potential damage from a cyber-attack.

Furthermore, having a managed SOC raises an organization's security maturity level significantly as it allows for stronger security of the organization's endpoints, network and cloud while providing around the clock monitoring, detection and response. By taking a proactive approach to security and finding threats before they penetrate and impact the organization, a managed SOC helps identify cyber incidents before they do damage in addition to speeding up the time to remediation should an event occur.

For the IT professional, having a managed SOC means you have a cybersecurity partner to lean on when an event happens. You can rest assured knowing that your digital assets and devices are monitored all the time, every day, year round.



THE BARRIERS

While many small businesses recognize the benefits of having their own SOC to protect their data, devices and people, most IT departments do not have one. Why is that?

In order to operate a SOC, an organizations needs to ensure 24/7 coverage. This is done through a combination of multiple (and often complex) cybersecurity technologies and an experienced team which includes SOC analysts, security researchers and threat hunters.

Cybersecurity technologies can be expensive and are traditionally complex, difficult to deploy and require massive efforts to maintain. This makes it harder for small IT departments to adopt these technologies, deploy them and commit for the long term.

Additionally, many small businesses lack the in-house security expertise needed in order to run a SOC and they often can't afford the investment and human costs associated with it. Security experts are expensive to hire, and those skills are relatively hard to adopt so training personnel from scratch is often not a valid option for a small IT department. Moreover, because security professionals are always in high demand, retaining them is also a challenge.

To operate a 24/7 SOC, you must have enough SOC analysts to provide full coverage. So, not only do you need to hire and/or train security professionals to analyze indicators of compromise and triage alerts, but you need enough of them to adequately staff a 24/7 operation even on weekends and holidays, which is no easy task.

Establishing an in-house SOC takes time and requires massive investment. As such, it should be a strategic decision that few would take. These barriers are high, leaving many small businesses exposed or looking for an alternative.

KASEYA MANAGED SOC

Designed specifically for a small business environment, Kaseya Managed SOC, powered by RocketCyber, is the ultimate solution for IT leaders who see the potential and value of providing a managed detection and response service to their customers but find the barriers of setting up a SOC practice too high.

Kaseya Managed SOC is a managed detection and response service that leverages RocketCyber's Threat Monitoring Platform to detect malicious and suspicious activity across three critical attack vectors: Endpoint, Network and Cloud.

Our team of cybersecurity veterans hunt, triage and work with our partners' teams when actionable threats are discovered. For more information about Managed SOC, please go to: ***https://www.kaseya.com/products/managed-soc/***

©2023 Kaseya Limited. All rights reserved. Kaseya and the Kaseya logo are among the trademarks or registered trademarks owned by or licensed to Kaseya Limited. All other marks are the property of their respective owners.