Key Reasons You Need a Security Operations Center (SOC) and Why You Should Outsource it.

The best way to define a Security Operations Center is as follows: A SOC is like the eyes and the ears of an organization, sounding the alarm when it detects anomalous, malicious or suspicious activities and, importantly, enabling the crucial response.

You may be thinking, you're too small or you have nothing worth stealing or that your firewall and anti-virus are enough. The harsh reality is that 43% of cyber-attacks target Small to Midsize companies,[1] 80% of companies experienced a cybersecurity incident in the past year [2] (many are unaware they were even attacked) and 70% of customers claim that they will stop doing business with a company after a data breach. [3]

The 5 key features of a SOC are:

Data Collection and Correlation: Your network, devices, security systems and cloud produce a vast amount of data. Getting all this data in one place, organizing it, and making sense of it, is a top priority for a SOC. There is also the important task of running regular vulnerability assessments across the network to identify systems and applications that are out of date

Proactive Detection of Malicious Activity: You don't want to wait the average 206 days it takes US companies to detect a breach. You want to know as quickly as possible to minimize the effect of the breach. The detection portion of the SOC includes anomaly identification, threat hunting and behavioral analysis to quickly find activity that is out of the norm.

Security Monitoring: SOC analysts constantly monitor for threats using their expertise, along with advanced security software and hardware. Here, the priority is triage: determining what alerts in your SIEM are important and which are false positives.

Incident Response: When threats are identified, the SOC's job is to move quickly to contain and remediate it. This is a complex task and requires many people, programs and processes to be in place.

Compliance Management and Reporting: Most aspects of compliance like PCI-DSS, NIST and many others are security focused. A SOC helps you meet, manage and maintain those requirements. SOCs even supply the reports needed to satisfy auditors.

1. https://www.prnewswire.com/news-releases/43-of-cyberattacks-target-small-businesses-300729384.html
2. https://www.bitsight.com/hubfs/White_Papers/BitSight-Forrester-Consulting-Study-Better-Security-Business-Outcomes-Security-Performance-Management.pdf
3. https://www.gemalto.com/press/pages/majority-of-consumers-would-stop-doing-business-with-companies-following-a-data-breach-finds-gemalto.aspx

The key benefits of a SOC are:

Risk Reduction – By reducing dwell time of threats from the average of 206 days, to less than 1 day, SOCs vastly reduce the chance that your organization will be badly damaged by a breach.

Peace of Mind – a SOC is like your eyes and ears, without it threats can sit undetected and you won't know they're present. By having a SOC, it's like setting the alarm on your house at night, it enables you to rest easy.

Reputation Protection – Your reputation is everything and you must work hard to protect it. These days news of a data breach at your company can spread in minutes online and in social media. In a recent survey, 70% of customers claim they will stop doing business with a company after a data breach.

Company Uptime – Cyber attacks like ransomware have the potential to shutdown your network for days, potentially costing you lost customers, productivity and data.

So why don't more companies have a SOC then? Mostly it's because of price. The hardware for sensors and software you need is expensive on its own. But pales in comparison to the people cost.

Here are 4 reasons to work with a Managed Security provider instead of building your own SOC:

1. Security Analysts are in high demand. There are far more positions open at companies than qualified people to fill them

The cybersecurity workforce gap is estimated to be growing, with the projected shortage reaching 3.5 million professionals by 2021.[4]

Bottom line, this is a very difficult position to find and keep filled, so let a Managed Security Services company deal with it for you.

2. Security Analysts command a salary of 6 figures. Are you willing to pay this cost for more than one security analyst? There are very few companies that committed internal staff to this task, and to do it right you need more than one dedicated person. Most businesses will delegate it to their best system or network professional as an additional job responsibility. This usually means that after a while of all being quiet, they'll let it fall to the wayside and focus on other job functions, leaving your network vulnerable to threats.

3. Keeping your security professional up to date and certified is a daily commitment. Are you going to keep this person(s) educated and give them the threat feeds necessary to understand what is coming your way on the internet? Are they going to have time to read about all the different threats that come into the field every day, filter through them, and figure out what may or may not be a threat to your business? Your SOC declines in effectiveness every day that this doesn't happen.

4. The threat intelligence gained from what you can see in your systems is limited. A Managed Security provider is seeing the activity in your environment and their other clients' environments. When a threat is discovered on one system, they can leverage this intelligence to proactively address on your system as well.

A SOC and security information and event management (SIEM) software backing that SOC is only useful if you have the people, processes and intelligence to maintain the tools and interpret the data turning it into useful information. This is not an extra duty, it's a full-time job.

Interested in implementing a SOC? Clearnetwork has been a Managed Security Services Provider (MSSP) since 2002, our expertise is in providing a fully managed SOC with excellent service and best in class threat intelligence and software all at a price you can afford. Our security analysts have a combined decades of experience and will work with you like an extension of your IT staff. Give us a call at **800-463-7920 x3** or email us at **sales@clearnetwork.com** to ask questions and/or schedule a demo. We also offer a free Proof of Concept so you can experience our powerful service for two or more weeks.

4.https://cybersecurityventures.com/jobs