WHITE PAPER

What is a SOC, and what benefits can we expect?

Gradient CYBER

Gradient Cyber is a trusted cybersecurity partner operating primarily across the United States and specializing in small and mid-market enterprises concerned about cybersecurity but lacking the staff to give it the attention it deserves. For a fraction of the cost of hiring one cyber analyst our cybersecurity team is on the job 24/7 to improve your security, so you don't have to think about it anymore.

972-532-1878 • contact@gradientcyber.com • www.gradientcyber.com

TABLE OF CONTENTS

INTRODUCTION

Businesses of all sizes today are highly, if not 100 percent, reliant on their digital communications infrastructure, making cybersecurity and 24/7 security operations a mission-critical capability for all businesses.

In the first paper in this series, we discussed the dramatic increase in cyberattacks in 2021 and 2022 and the impact on businesses. The need for increased security, meeting compliance mandates, addressing supply chain risks, better utilizing existing security products, and preparing incident response capabilities is driving businesses to create a Security Program and make use of a Security Operation Centers (SOC) in some form.

However, once a business understands that cybersecurity is critical, it can quickly become overwhelmed by the amazing array of security services, products, and capabilities available. With more than 3,500 cybersecurity companies[i], it can be almost impossible to understand which products and/or services are best suited for your organization. Even the most informed users struggle to evaluate and select from the entire set of products and services.

Given this complexity, many companies work with Managed Security Service Providers (MSSP's) who can assist with evaluating and selecting security offerings. These MSSP's offer security services to support many of the leading security products. That said, with more than 250 MSSP's[ii], it can also be difficult to select an MSSP given the array of services (and products) offered.

When working with an MSSP, many companies initially use the MSSP to help setup a security program and a Security Operations Center (SOC). Per Figure 1[iii], 98% of MSSP's surveyed said they offer a SOC of some sort to their clients.

The downside to such an array of choices in SOC vendors, is that the resulting matrix of possible features is difficult to understand and even harder to select from. To further complicate the evaluation process, analysts and vendors have created new markets and sub-markets that define various features that can be hard to differentiate. For example, a quick search of SOC providers will yield a large number of SOC providers, Managed SOC providers, SOC-as-a-Service (SOCaaS) providers, Managed Detection and Response (MDR) providers, and Extended Detection and Response (XDR) providers. To make an informed decision, enterprises must understand these offerings, and their key features and value propositions.

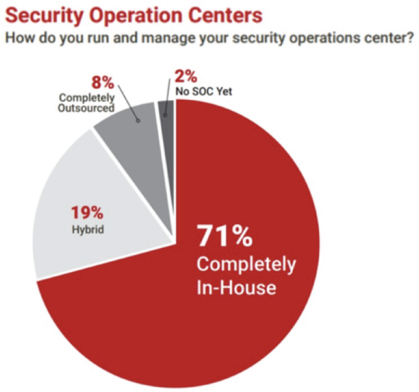

Figure 1 - MSSP's that support SOCs as reported by "MSSP Alert Top 250."

SO MANY SECURITY SERVICE PROVIDER ACRONYMS

In recent years the acronyms being used to describe security services have proliferated. Below we list some of these acronyms and their nuanced meanings. Instead of getting distracted by the names and abbreviations, that at the end of the day add little value, the reader should quickly endeavor to get past these labels and evaluate service providers on the primary features that matter most to them.

Now let's discuss the names and acronyms. Built on-top of basic monitoring, many SOC providers add additional technologies and capabilities. The various service and product names, and their associated acronyms, make for a confusing market landscape. All of the SOC-centric service offerings described below reflect a service provider's efforts to provide outsourced / managed services that address a customer's cybersecurity monitoring need.

- **Managed Security Service Provider (MSSP)** - This term refers to almost any vendor that provides any level of security services. Historically, it defined a security services organization that outsourced security program development and security product management. In this initial definition, it typically stopped short of threat detection and response capabilities. However, many MSSP's are now adding threat detection and incident response capabilities to their portfolio as Managed Detection and Response (MDR).

- **Managed Detection and Response (MDR)** - This offering typically provides SOC functionality on specific technologies only, offering some form of additional threat hunting and incident response capabilities on top of the ability to monitor and detect threats. In many cases, product vendors view MDR as a value-added service to their endpoint security or network security product. Using the advanced features of those products to allow the vendor to offer a 24x7 monitoring service and specific threat hunting and response capabilities limited to those products. Many of the most popular MDR providers offered the service as a Managed Endpoint Detection & Response (Managed EDR) service, building services on top of their existing endpoint security product or as a Managed Network Detection and Response (NDR) service, building services on top of their existing network monitoring product. That said, MDR has been increasingly offered as a next-generation managed SOC offering by general security service providers with support for an array of technologies.

- **Managed SOC** - This term is generally a subscription-based service offering whereby customers outsource threat detection and response. It generally provides SOC functionality, as described above, but can also include proprietary tools and processes to make the capability operate as a customer-centric service. For example, most managed SOC's offer a situation report / event tracking platform that allows the customer to interact with SOC analysts and obtain important reporting and security posture updates.

- **SOC-as-a-Service (SOCaaS)** - This term is generally another name for a managed SOC.

- **Extended Detection and Response (XDR)** - This offering is provided as a SOC service that extends MDR services across multiple types and layers of technologies. Where many MDR solutions focus on a single technology type (often EDR or NDR), XDR implements the analysis, detection, threat hunting, and response capabilities across multiple types of products including the network, endpoints, servers, SaaS applications, and cloud. Some security product vendors offer their XDR services only for their specific products, while other SOC providers offer XDR generally across a broad range of products.

While there may be distinct differences between each of these different SOC-centered offerings, the differences are nuanced and not generally clear.

It is not possible to pick a SOC services vendor solely based upon the acronyms they use. Instead, the reader must go past the labels and evaluate the primary features that matter most to their organization.

WHAT DOES A SOC DO?

Researching the capabilities of a SOC yields a broad array of answers that all revolve around the concept of providing people, processes, and technology for the purpose of monitoring and responding to security issues. In most cases, a SOC exists to monitor your organization for security events and respond to cybersecurity events.

In this document, the intent is to describe the capabilities that are commonly provided when an organization is seeking to hire a managed SOC to manage and monitor its cybersecurity events. In order to normalize the discussion, this conversation will focus directly on services that are made available through Managed SOCs, that offered shared SOC services to many clients, as those capabilities are generally aligned to the needs of small businesses and midsize enterprises.

When an organization is searching for a SOC, they generally are looking for a cybersecurity monitoring solution with the right set of tools and products that match their unique needs. These needs vary widely and can include a broad set of security technologies. Thus, vendors have created a variety of marketing labels that are used in conjunction with the term SOC. The following sections discuss the purpose of a SOC and how the market addresses the various features.

A **Security Operation Center (SOC)** is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

A SOC acts like the hub or central command post, taking in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside. The proliferation of advanced threats places a premium on collecting context from diverse sources. Essentially, the SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC must decide how they will be managed and acted upon.

MONITORING YOUR SECURITY

In general, everything in a SOC is centered around monitoring and responding to security events, as described above[iv].

A SOC is always enabled with a mechanism for the collection and analysis of security events. In most implementations, the SOC uses a Security Information and Event Management (SIEM) or similar platform that collects log data and network telemetry from various sources, normalized and analyzed to detect security events[v]. In some cases, the SIEM product is purpose-built by the SOC provider. The SIEM is configured to receive log messages and data from security products that exist within the monitored IT environment.

Built on-top of the event collection system, the SOC constructs the processes and supplies the expert talent to evaluate and respond to security events that are detected. The processes and tooling used by the SOC analysts is a critical aspect of the SOC's ability to provide strong security monitoring. Further, the SOC team typically builds proprietary "runbooks" or "playbooks" that detail the steps that analysts follow for various security alerts.

The ability to monitor, detect, and respond to security threats is the key function of the SOC for your organization.

FEATURES THAT MATTER

Regardless of whether you have been searching for a SOC, SOCaaS, MDR, or XDR, you are likely searching for some key aspects of those services that will protect your business. Below is an aggregated list of SOC features from vendors, analysts, and Gradient Cyber customers to look for when evaluating managed SOC solutions.

- **A Trusted Partner** - First and foremost, when selecting a managed SOC (of any type) partner, you are selecting an organization that you are going to rely on to keep your business safe. You are depending on this team to monitor the technologies that protect your critical systems and data and to have the expertise and advice you need to make smart decisions in times of crisis. It is important to be able to form strong relationships with the leaders that will be communicating with your IT team on the discovered security events and that the SOC team makes time for periodic reviews and discussions on the security of your environment.

- **Fit for Purpose** - In evaluating a service offering, for your small business or midsize enterprise it is important to make sure that the offering is scaled correctly for your size, that you will receive the same attention as much bigger customers, and that the SOC services and pricing model will easily scale with the needs of your business over time.

- **Leading-Edge Technology** - It is important that your managed SOC provider focuses on building and supporting leading security technologies. As your trusted security partner, they should provide mature technologies to identify security vulnerabilities, detect advanced threats, and respond to both. Your managed SOC partner should also be flexible enough to support your existing security technologies.

- **Technology Agnostic** - Some managed SOC providers support only a narrow endpoint, network, and cloud protection technology stack, in order to ease their burden of supporting various solutions. These limits may constrain your ability to select the right security products for your environment. Carefully evaluate what level of vendor / solution lock-in your organization is willing to accept.

- **Deep Cybersecurity Expertise** - Look for indicators that the SOC leadership team has the expertise you need to identify and respond to threats as they occur in your environment. Customer referrals are a great source to understand whether the partner's security expertise is providing value to their clients. Also look at the security certifications and training the SOC team members maintain. And lastly consider the stability or conversely the turnover of the SOC team and analysts that will monitor your IT environment.

- **Regular Team Interactions, Meetings, and Reporting** - As you build your relationship with your trusted security partner, it is important that there are regular and periodic touch points that can be used to discuss and review the security of your environment. Receiving regular written reports on the activity of the SOC, as it relates to your environment is also important to make sure you have visibility into the efforts being made to respond to events that are generated by your infrastructure. This also serves to cross train your internal teams and mature your own capabilities.

- **Threat Hunting and Response Capabilities** - Regardless of whether your managed SOC is referred to as an MSSP, SOCaaS, MDR, or XDR, it is important to confirm that your managed SOC offers the ability to hunt for active threats within your environment and to respond (contain) those threats, once identified. Ask your provider to describe their threat detection, hunting, and response processes in detail, to understand the steps their analysts follow to help protect your environment.

- **24/7/365 Cyber Analyst and Security Monitoring Coverage** - Look for managed SOCs that do not limit the coverage time or severely limit the number of analysts working per customer. These limitations can reduce your organization's ability to recover from critical security events or result in excessive false positive events that your team must action. 24/7/365 SOC coverage and human-in-the middle cyber analyst response is a critical requirement for an industry leading SOC.

- **Monitoring Your Entire IT Environment** - As cyberattacks can impact any aspect of your IT environment, it is important to make sure your managed SOC can monitor as many ingress points as possible. Managed SOCs must at a minimum be prepared to monitor your network security, endpoint security, email security, domain controllers, and web security tools to maximize your visibility and protection. You may not start with monitoring the entire IT environment, but make sure your partner can expand your security monitoring if and when you require.

- **Active Response Options** - Traditionally, managed SOCs provided only 'passive' security event guidance as a response. In this case it is up to you to take all the necessary security event response steps to contain and eliminate the threat. Now SOC providers may provide your organization with active response taking proactive action to speed security event response times and lower workload on your internal IT/security team.

- **Cybersecurity Health and Compliance Evaluations** - To fulfill their role as a trusted security partner, it is important that your managed SOC has the expertise and capability to help evaluate all aspects of your business to confirm that you have deployed the appropriate security products, controls and frameworks for your industry and company size. Being able to perform these assessments is important to providing the holistic cybersecurity support that organizations require.

- **Local Intrusion Detection System (IDS) Support** - A solid security program provides multiple layers of protection for your environment. In addition to collecting security events from your firewalls and network security devices, it is important that the managed SOC offers an additional level of local Intrusion Detection that is fully available to their analysts for correlation and investigation of events that occur. This layer of support is critical in allowing the SOC's expert analyst a deep level of visibility in providing threat hunting and response capabilities.

- **SIEM Provision or Support** - Managed SOC providers may provide a proprietary platform that includes SIEM functionality or they may simply manage your existing SIEM (if you have one). But some form of SIEM is required to collect, correlate and analyze threats as they appear in your environment. Think through whether you need your own SIEM or if you will use the managed SOC vendor's platform and keep in mind the extra cost if you decide to purchase your own SIEM.

- **Integrated Threat Intelligence** - Threat intelligence sources provide external feeds of information that let your security team know the details of ongoing cyberattacks in the wild. It is important that your managed SOC integrates these data-feeds into their tools and processes, in order to provide strong correlating details in threat hunting and event analysis for your team.

- **Cloud-Based Security Operations Platform** - To effectively support a managed SOC service, your provider should provide a cloud-based platform to, at a minimum, track the maturity of your cybersecurity health, aggregate data and detect threats, and immediately communicate ongoing event investigations. Further, the platform should optionally allow your team to interact directly with your SOC team for events in progress.

- **Asset Discovery** - To properly monitor and investigate issues as they occur, it is important that your managed SOC includes a process for discovery and classification of the devices that are interacting in your IT environment. This discovery process not only identifies systems that should be monitored but also helps the SOC to classify the purpose of each system to help understand expected and anomalous behavior.

- **AI/ML and UEBA** - To stay on the leading edge of security protection technologies, your managed SOC should be integrating the leading Artificial Intelligence (AI), Machine Learning (ML) and User and Entity Behavior Analytics (UEBA) into their SOC platform. These analytics tools are available for integration into most SIEM technologies and provide the SOC's analysts with the capabilities to expedite the detection and discovery of active threats. SOC's that do not implement these technologies risk providing a lower level of quality to their customers.

- **Elimination of False Positives** - From a day-to-day perspective, one of the most valuable aspects of a SOC is the work that their cyber analysts perform to analyze security events and eliminate false positives. SOC providers that offer only automated evaluation and delivery of aggregated logs to their clients are not providing SOC services, they are providing a Managed SIEM. The design of security products today generates a significant number of events that end up being classified as "false positives" upon review within the context of your environment. Outsourcing the expert evaluation of events and reducing the total number of events your staff has to review is a must-have feature of an managed SOC.

BENEFITS OF A SOC

Now that we have discussed the operation and key features you should expect from a managed SOC, it is important to now connect all those capabilities to the benefits a business should expect. In totality, these benefits will provide the strong security expertise, on top of your existing IT and security infrastructure, that your organization requires to be protected against and respond to cyberattacks.

Trusted Security Expertise - Cybersecurity has become a business-critical skillset required for your enterprise, similar to accounting or IT. When selecting the right SOC provider, you are selecting your trusted partner for protecting your organization from security threats. The right partner will bring extensive knowledge and experience in the cybersecurity industry, assessing your current cybersecurity health, the active threat landscape, and the current best practices in protecting enterprises from threats. The experience and capabilities of your SOC team will play a key role in allowing your company to focus on your core business.

Improving Your Current Cybersecurity Posture - A trusted managed SOC partner should do more than find and fix cybersecurity threats – they should evaluate your current security program and your current cybersecurity practices and work with you over time to implement a roadmap of recommendations to improve your cybersecurity posture. In the long run these improvements reduce your business risk; protect your business; customers, partners, and employees; and reduce the cybersecurity workload on your IT team.

Reduction of Work for IT Team - A well-functioning SOC will manage the security alerts that are being generated by the various security products that have been deployed by the company's IT team. In their analysis they provide the expertise to eliminate false positives and dramatically reduce the number of alerts that need attention from the company IT team. They may also take action on behalf of your team with active response capabilities. These efforts will relieve the IT team of the significant burden of managing those events, while providing additional expertise that does not exist within most IT teams.

Security Event Escalations - In the unusual case that a security event should be escalated to a security incident that can pose significant harm to the business, it is critical that your team has access to experienced professionals that have the tools and capabilities to help guide your organization and respond to the threat. Your managed SOC partner will have the expertise to identify those threats and to support your efforts to contain.

HOW MUCH ARE WE TALKING?

Unfortunately, there is not a single answer that can be applied to all enterprises to help understand what the cost will be for managed SOC services. The total services that you decide to take advantage of, combined with the company's risk profile has an impact on the services required and therefore upon your price.

That said, the industry does put forth some general guidelines that can be helpful in considering a reasonable level of spend, compared to other small and medium sized businesses. Many industry observers point out that, in general, cybersecurity budgets for small and mid-sized businesses fall in the range of 6%[vi] to 15%[vii] of the total IT budget. Depending on your organization's risk appetite, you can decide where your organization should fall within that scale.

Once the total annual security budget target has been identified, you must determine how much of that budget should be allocated for security products and tools, versus security services. Services provide a cost-effective approach to accessing hard-to-find security expertise for smaller businesses. Overall, small and mid-size businesses should expect that they leverage at least 50% of their security budgets for outside services. A small business would likely leverage all of the services budget for managed SOC services.

These numbers can provide a starting place in considering your target budget for a SOC. What you end up needing to pay should also be reflective of the infrastructure you are monitoring. The right managed SOC partner will offer a variety of options to help build a package that fits your risk profile and maximizes the value obtained for your available budget.

NEXT STEPS

With the wide array of SOC capabilities and features that are available, the SOC evaluation and selection process can be quite challenging. Most of all, it is important for businesses to realize that when they are selecting a SOC, they are entrusting that company with the security of their business. Selecting a trusted partner that you are confident will be vigilant in monitoring your systems and provide the strong expertise needed can make the ultimate difference in surviving a cyberattack.

See white paper #3, titled "How Do We Build a Business Case for a SOC?" in which we provide guidance on how you can put together a plan and business case for your organization's investment in a SOC.

---

i Momentum Cyber Cybersecurity Snapshot February 2022

ii MSSPAlert Top 250 MSSPs, 2021

iii MSSPAlert Top 250 MSSPs, 2021

iv What is a Security Operations Center (SOC)?

v Gartner Information Technology Glossary > Security Information and Event Management

vi Cost of Cybersecurity in 2021

vii How Much Should I Spend on Cybersecurity?