**How Much Do Managed Security Services Cost?**

When it comes to managed security service providers, a wide range of services can be offered, from vulnerability management and penetration testing to security operations services. This article will focus on a specific category of managed services, detection and response. It will further break down the services into three key categories, all focusing on different detection capabilities: managed detection and response, managed cloud security, and security operations center.

With all the different types of managed services available, it can be difficult to know which type of service an organization should choose. This is no different when it comes to the three types of services that will be discussed in this article. To help decide the correct service for your organization, this article will break down the scope for each of these service offerings, some cost factors, and will dive into a review of real work pricing examples. With this information, along with a few tips and tricks, your organization will be able to decide on the right service and partner for your organization’s needs.

**Scope for Managed Security Service Providers**

When it comes to managed detection and response, managed cloud security, and security operations services, it can be difficult to fully understand the differences between these services. It can be especially tough when considering the overlap between the three services and the sheer number of vendors and consultants that claim they can instantly protect your organization. During this section, the scope for each service will be discussed to help better understand exactly what these services are providing. Finally, a quick overview of how these services may operate together to better secure an organization.

**Scope for SOC**

Security operation center services are the oldest solution of the three offered by security vendors. This service initially started out as running or managing security incident and event management (SIEM) tools for organizations. Since this time, it has evolved to be a bit wider in the capability to take on new and emerging tools like Sumo Logic or Spunk, which provide SIEM-like capabilities with more robust logging solutions. When evaluating this solution, the typical offering involves building alerts, managing alert triage, and providing the organization with alerts or events that may require further investigation or remediation. A good rule of thumb is to consider that this service typically provides tier 1 level support, which can help lower the overall noise for an organization but may not provide much in the form of remediation.

**Scope for MDR**

When it comes to managed detection and response, this is the natural evolution of the SOC service. This service aims to help close the gap many organizations have related to security skill sets in the organization by providing threat-hunting and remediation-type services. This service will focus on managing alerts, remediation of alerts, and to a certain extent, threat hunting capabilities. When engaging vendors for this service, it is critical to understand that the scope can be as broad as providing MDR for full enterprise logs to just providing endpoint MDR services. It is critical to keep in mind the end goal of what your organization is wanting to accomplish or what gaps your organization is looking to close.

**Scope for Managed Cloud Security**

This service may seem straightforward based on the name, and for the most part, it is. Managed cloud security not only provides detection services but will also often augment with additional services related to cloud management and configuration monitoring. In addition, it can also provide services related to infrastructure as a service cloud solution provider (AWS, Azure, etc.) to SaaS-based services like O365 or GSuite. So, while the name may make it seem like it is a straightforward service, understanding the cloud-based scope your organization needs assistance with is critical when evaluating vendors providing this service.

**MSSP Cost Benchmarks**

When it comes to pricing for these three services, they can vary greatly depending on the size, complexity, and scope of the contracted services. The two biggest buckets that a vendor or service provider will be most concerned with is tool cost and internal people/employee time required to assist their clients. With this in mind, we can attain a high level of understanding of what the service providers are trying to understand when it comes to pricing for an organization. Below are some quick examples of pricing for organizations:

For an organization contracting for MDR that is a technology company looking to contract for endpoint services with a total workforce size of about 500 it could be between $50,000 to well over $100,000 per year.

For the same organization to attain cloud security services, the total cost could be north of $100,000 a year.

For a SOC service that does not include remediation services, the cost could be $150,000 to $300,000.

**Cost Factor #1: BYOT or Provided**

An organization might think that providing their own tools (BYOT) will allow them to be more cost-effective than working with a provider that will take on the licensing cost for the tool(s) required to provide the service. However, this is not often the case. In many cases, there is a scale of economy that can be taken advantage of by purchasing tools through a company that is also providing the service to manage and monitor those tools. Due to the sheer number of licenses that the vendor may be purchased across clients, the overall cost from the partnership with the vendor can be significantly lower than the cost for an individual company to purchase. Keeping this in mind for a managed SOC, MDR, or cloud security can be helpful to help manage costs for an organization.

**Cost Factor #2: Number of Assets**

Calculating assets is one of the most common ways for a vendor from any of the three services to get an estimate of the total amount of work that may be required to help manage your security tools and alerts. The total number of assets will relate to a potential number of security misconfigurations, alerts, or events that may require human hours to assist with evaluating, which is one of the biggest cost components for any vendor providing services. Depending on the service, this could be the total number of endpoint systems, servers, containers, serverless functions, or network/firewalls in the environment. Unfortunately, this mechanism for pricing does make it difficult for an organization to fully understand potential cost, as it relates to organizations of similar population size. For example, a technology company may have a larger number of total assets than a company in logistics of the same size.

**Cost Factor #3: Remediation Services**

While MDR and Cloud security often include remediation services as part of the pricing, it is not always guaranteed to be added. If your organization is lacking the internal capacity or capabilities to manage security events after they happen, it is worth discussing what type of remediation or ‘fire’ services the potential vendor can offer your organization. As is the case with other factors, the biggest risk in profitability for a vendor is the amount of time they will potentially need to provide from people interacting with a customer. So, when it comes to this factor, expect it to add significant cost to the overall price of the service. Spend time evaluating the cost for your organization to hire and train a person to take on these responsibilities vs. having this capability outsourced.

**Cost Factor #4: Scope of service**

The last cost factor is a large bucket. As addressed in the scope section, each one of these services can be nuanced in what they are offering. If the service is focused on full enterprise MDR, the price will be significantly higher than if the primary focus is just on endpoint management. This can be similar for cloud security services for infrastructure-as-a-service type offerings that would consist of fully hosting monitoring vs. managing a SaaS application like O365. This factor may be one of the biggest cost drivers on this list and can easily add six figures to the total contract value once the scope has been determined by the organization.

**Real MSSP Cost Case Studies**

When it comes time to contract for any one of these services, it can be hard to know what to expect on the total contract value. While the two case studies below will provide a very wide range of costs without added value, it does provide insight into how the cost can vary from a large organization to a smaller organization. Unfortunately, the total dollar cost of a service can grow quite quickly for a complex or large organization, but one of the best tools your organization can use when evaluating the ROI is to evaluate which licenses are included and how many people it may take to operate the same capabilities internally.

**Case Study #1: Large SOC Service**

**Industry:** Logistics - Energy

**Size of the Organization:** 3,000+ Employees

**Scope:** Security operations center to manage tier-one alerts across the full enterprise

**Cost:** $2,000,000 in year one with escalating cost as additional logs were ingested

**Description:** The service was focused on providing a build and operation of a 24x7 security operations center that provided tier 1 alert and event triage capabilities for a multi-national organization. The organization had an internal security team that was capable of investigations and threat hunting in the environment but lacked the staff to fully manage a large complex enterprise technology security monitoring capability.

**Additional Details** Initial logs focused on endpoints detection and response, network, firewalls, AWS, and existing servers on-premises. The eventual goal was to ingest OS-level logs from all endpoints, servers, and containers running in the environment.

**Analysis:** There may be some sticker shock with this case study, but the volume of logs that the company was going to be ingesting was quite large. To further understand the cost, the service provider was also providing the primary logging and SIEM-like solution for the organization, which could easily have accounted for half or more of the total year once cost for this company. Additionally, there were options, or escalators, in the contract for the service provider to take on threat hunting and remediation services once the full solution was fully operational. However, at the beginning, the contracting organization decided to keep those skills and costs in-house.

**Case Study #2: Broad MDR Service**

**Industry:** Technology

**Size of the Organization: ~**100 employees

**Scope:** SIEM, Email, Phishing, Training

**Cost:** ~$60/month per user, ~$75,000/year

**Description:** A fairly young technology company contracted with a vendor to provide an MDR solution that consisted of monitoring endpoints, email services, phishing, training, and infrastructure monitoring. The vendor provided alert and event monitoring, along with remediation services, for most of the alerts or events for the organization.

**Additional Details:** The organization did not have the capacity to hire a team of security engineers or analysts to build and manage the various tools that would be required to build the initial security operation capabilities. The vendor was able to provide a few additional capabilities beyond what was needed, at the same cost for the organization.

**Analysis:** This was a full MDR solution for the enterprise with the ability to add on additional, more in-depth cloud security solutions later for about $20 per user per month. The vendor for this service is attempting to keep the pricing model simple by basing it on the total number of employees or users in the organization, which makes it easier to understand the cost of the contract.

**How Much do Costs Vary from One Vendor to The Next?**

As is the case with any security service, price or cost can vary drastically from one vendor to the next. In this particular case, there are so many variables that lead to the pricing variation that any organization may encounter. Keep in mind that many of these variables are not direct indicators of how well an organization can help manage alerts, triage, or remediation of your security monitoring solutions. If in doubt, ask for references to better understand the capabilities of the vendor.

First, are the resources based in the country, near shore, or offshore? Obviously, an organization operating with resources based in the US vs. those based in India will have two separate pricing models. While these services are becoming more tool heavy, the reality is that any one of these services is still very heavily reliant on people to operate. This particular factor may have the largest impact on total contract value.

Second, the tools that are being used as part of the service must be considered. For example, for cloud security services using Prisma Cloud vs. Ermetic may very well have a large difference in pricing, due to the overall cost of the tools. This is not to say that either tool is better than the other; it’s all in how they are used and managed by the vendor. Keep in mind that finding a vendor that uses more cost-effective tools may be a great way to help reduce the cost of the overall solution.

With these two factors in mind, it can help explain why the cost for the same service from one vendor to another can vary as much as six figures. The more complex \_\_\_\_\_\_ or number of total assets in the environment, the more your organization may see the total cost vary from one vendor to the next. Even those the cost may vary significantly from one vendor to the next, there are ways to help manage the overall cost of the contract.

**How Can MSSP Costs Be Reduced?.**

When it comes to MSSP costs, there are not a lot of ways to reduce the overall cost. Keep in mind that anytime your organization is looking for more eyes on glass capabilities, the cost will increase quickly, as this requires investment by your vendor in personnel. However, there are some tips that can be used to help manage the upfront costs to the organization:

* Ramp up – Rather than buying or contracting for everything that your organization would like to monitor from the start, focus on the most critical components to start with. Ramp up over the next year or a few to allow for the business to continue to grow to support the additional costs. This also provides your organization the ability to determine if everything needs to be fully monitored by your vendor.
* Bundle tools – It may not be ideal to have to retool to work with your preferred partner, but it may very well be likely that if you retool your licenses under your vendor, you can save money. Keeping in mind that most vendors will be able to have large discounts that your organization may not be able to attain, this is a great way to help lower the overall security budget.
* Hybrid – If your organization already has an internal security team, consider a hybrid approach. Maybe your vendor only provides off-hours help. Or maybe they help tune the environment for your internal team rather than fully monitoring. Most vendors in this space are willing to customize their approach to help manage the cost for their customers.

**Costs of MSSPs Vs. Benefits**

There can be multiple benefits when engaging an MSSP to provide any one of the security services discussed in this article. Whether or not these are benefits to your organization depends on the maturity, size, and capabilities of your organization. For example, a startup will gain nearly all these benefits by engaging a third party, while an organization that is highly mature and has sufficient resource investment may not gain any of these benefits. The following are benefits that can be attained by contracting with a partner to provide the selected services:

* Close the skill gap – Even in the current state of the workforce, it is still extremely difficult and expensive to hire appropriately skilled security practitioners.
* Bolt on tools – Working with the right partner, a whole suite of tools may very well become available that otherwise would require significant investment across multiple vendors.
* 24/7 alert management – Gaining the ability to have more robust monitoring and triage with needing to hire for overnight or overseas can be an extremely beneficial value
* add for an organization
* Herd defense – This one may not come to mind for most organizations but hiring a vendor to provide these services can provide a herd defense capability. The vendor/partner will be able to apply rules, alerts, and preventative policies across clients based on what they are identifying from any single or multiple clients in real-time.