Introduction

An MSSP, or managed security service provider, is a specialty managed service provider, which provides an outsourced security solution for a client, rather than more general work related to IT or telecommunications. The core of what an MSSP offers is contract-based longer-term (more than a few weeks) security services to assist organizations with projects, ongoing security program management, or operational support for an organization.

Over the years, MSSP have gained popularity for a myriad of reasons. One of the largest is due to the overall shortage of qualified cybersecurity personnel. Other reasons for this include a need for security to be implemented and matured in organizations of all sizes, which places a large financial investment requirement on smaller organizations. This has rapidly increased the demand and market for MSSP to provide outsourced security services to smaller organizations on their path to cybersecurity maturity. In the short term, it is likely that there will be no decrease in MSSP providers or solutions that are available. It can be argued that we will only see an increase in MSSP providers with new specialty fields emerging, such as Metaverse, crypto adoption, and other technologies.

Common Types of Service Providers

There is a nearly endless list of services which a cybersecurity consultancy company could build an MSSP offering around. If there is a potential to generate recurring revenue with a client, a consultancy will build and bill for that service for a client. However, there is a whole list of common services that most organizations are leveraging as part of their MSSP ecosystem.

* Security Operations

This may be the most common service to date. This service can run the gamut of simply providing first-level alerting and review all the way to a 24/7 full-featured security operations center capable of hunting, triaging, and remediating alerts or indicators of compromise within your organization. In addition to providing monitoring services, some consultancies provide a resale add-on value to customers by bringing in their preferred or own SIEM and logging tools to further provide value to their customers. This service varies greatly from one provider to the next, both in service offering style but also maturity.

* Cloud Security and Management

With more companies moving to the cloud and the lack of slowdown of adoption of cloud-based solutions, this service continues to grow in cruciality for organizations. This service typically entails providing guidance on building secure services or applications in cloud solution providers or reviewing and managing existing environments. In this particular offering, the MSSP typically brings security consultants to your organization that has deep cloud computing security experience to help close the internal gap for your organization.

* Vendor Management

Every compliance framework requires a proper vendor management program. Almost every organization can struggle in managing its vendors. For this service, the MSSP takes on the role of reviewing new and existing vendors and providing recommendations on any mitigating controls that are required. This is a great service to offload significant work and potentially leverage herd knowledge from the MSSP provider.

* Compliance and Audit

While some of the security compliance frameworks will not allow a third party to manage a security program, this is still a high value add solution from MSSPs. This service may entail building a security program to meet a security framework all the way to acting as an internal audit to assist with managing highly complex compliance requirements for an organization.

* MDR

Managed Detection and Response, not to be confused with security operations (SOC) managed services are often a service or capability of a SOC solution. This service specifically deals with managed endpoint security detection and response tools. These tools provide information and alerts on endpoint security events, whether malware or suspicious network traffic. In many cases, the MDR solution provider is adding additional value in triaging and remediating alerts on the endpoints, while also providing off-hours support and monitoring.

* Network Management – Firewalls, WAF, IDS/IPS

In many cases, managing security tools and their configuration for network traffic can be tedious and mundane. This service is really offloading the management of requests, alerts, and operational monitoring for network security tools. This can be for physical devices that are deployed in a data center or virtual devices run out of a cloud service provider.

* Vulnerability Management

If an organization were to invest in one capability to rapidly mature and improve its ability to resist a malicious attack, it should be vulnerability management. This service encompasses vulnerability scanning, patch management, and remediation management of vulnerabilities and misconfigurations. Much like security operations managed service, this service will often come with tools or software as part of the service.

These are just a few of the services that can be contracted. Further services that are not detailed above could include penetration testing, security consultation, configuration management, and many other types of services. The reality is if your organization is working a security project and does not have the internal staff, it is likely that a security consultancy will provide a service as an MSSP to assist with completing the project.

Benefits of an MSSP

Not all service solutions provide the same level of value or benefits to an organization. For your organization to understand the benefit that an MSSP may provide, it is important to evaluate the needs, goals, and internal capabilities your organization currently has. Some of the biggest benefits that MSSP can provide are related to transferring risk and capabilities to a highly skilled partner to allow for internal resources to focus on other tasks. However, this is not the only benefit or value add that an organization may attain from engaging an MSSP for services.

Further benefits could also include, but are not limited to:

* Specialty Skills: It is not easy to hire resources, especially if it requires specialty or specific skills. A great example is related to cloud security, IoT, and block chain security. These are not skills that are readily available and can be hard to find and retain.
* Staffing up or filling the vacancy: Hiring and retaining security resources can be difficult. Utilizing an MSSP for operation security tasks will help eliminate the impact of having security resources exiting the organization. While your MSSP may have turnover, usually this has little to no impact, due to contractual requirements to provide the service or the lack of a single resource being assigned but rather a team.
* Build or mature security programs: There are builders and maintainers in the security industry. If your organization is looking to build or mature your existing security program, it may be a benefit to engaging an MSSP to help with this process, as your organization will not need the skills or capabilities for the long term. This provides the ability to meet your goals without having to worry about a security resource not being happy in a maintenance role.
* Monitoring or response capabilities to extend coverage time: There are many reasons to outsource anything related to security operations or alert monitoring for your environment. The biggest is that it is the easiest way to increase the active monitoring hours for your organization. Rather than having your internal team on call every few weeks, this could provide the ability for immediate triage and containment of an incident, while ensuring only the most critical items are escalated to your internal team.
* Operation support: This last benefit is encompassing a lot of different benefits. Operation support could be specific to a unique project that will not be an ongoing project or requirement. For instance, it could be to provide support for migration to the cloud or standing up new network security tools. Additional operational support benefits could entail taking on repeatable tasks, like vendor review, tool maintenance, tuning, or decommissioning of old tools or capabilities. Removing daily or unique operational tasks from your organization's internal team will allow them to focus on work supporting the business and being more responsive to new projects.

Tips on Choosing Managed Security Provider

With all of the different MSSP providers that are available to choose from, it can be overwhelming to decide on the right MSSP partner for your organization. When evaluating your partner MSSP, there are a few things that can be taken into consideration to assist with finding the right partner for your organization.

Expertise

This may be one of the biggest missteps that organizations make while selecting their MSSP. No matter how strong a reputation MSSP has, if they do not have the expertise or work with your technology stack, it will be tough for them to provide full value. A great example of this is related to cloud security. Google Cloud, AWS, and Azure are all cloud environments and have the same concepts in play, but they all have extremely unique services and controls that can be utilized. While it is possible to have an MSSP that is extremely experienced in Google cloud to provide services in AWS, the possibility is high that your organization is going to be paying your MSSP to learn on the job. In most cases, when hiring an MSSP, your organization is looking for value and benefits from day one. In this case, it will be delayed.

Technology Alignment

This is almost a subpoint under expertise but deserves to be its own tip. In many cases, your organization will have a preexisting technology stack deployed. Engaging an MSSP that is capable and knowledgeable in your technology stack will be critical for success. Especially when working with security operations or MDR solution providers, it will be important that they are familiar with your technology, as each solution performs a little differently. Another reason to be aware of the technology solutions the potential MSSP works with on a regular basis is that when they are deep expertise, they can provide out-of-the-box recommendations on how to best manage and configure that technology.

User Experience or Engagement

At first, you may not think that this is of high value or a component for selecting an MSSP, but it really is. How you engage, when you engage, how you track, and how you consume information from your MSSP is going to be vital for a continued strong relationship. Do you want to have a recurring weekly meeting, or would you prefer to have a porta from which you can attain information?

Responsiveness

Not all managed services need to have lightning-fast response times, but there are services that responsiveness will be critical. Evaluating potential partners on their willingness to commit, in contract, to SLAs related to response times would position your organization well to attain the response times that you need for the service. Some MSSPs will not commit to anything faster than 24 hours, which may not be acceptable for your organization. Consider if the service will potentially cause blockers for internal teams, if the response is over 24 hours. Causing friction within the organization may not allow your MSSP to provide the full value of the service and may just result in that work being placed back on your internal team.