

11 Elements of a Successful Managed Security Partnership

By Steven Drew

More and more organizations are turning to Managed Security Services (MSS) to help them achieve their security objectives. Security teams need to do more to protect their environment, but are facing a variety of resource constraints. A Managed Security Services Provider (MSSP) will remove some of the mundane operational activities so security teams can focus on strategic security initiatives that will deliver short and long-term benefits to their organization. Additionally, the provider is adding value by delivering timely security intelligence, real-time enterprise-wide monitoring, and device management that enhance the organization's security posture.

Selecting a Managed Security Service Provider is one of the most important decisions a security team will make. Choosing the right partner will often determine the success or failure of the initiative. The following information highlights the most important factors to look for when evaluating an MSSP. Since a provider is meant to be an extension of an organization's security team, they must be strong across the three fundamental areas of security: People, Process and Technology. Organizations should consider the following factors to ensure a successful partnership.

People

Like any other discipline, people are the most important part of a security program. A provider must have talented people analyzing events, managing devices and guiding the company. A company evaluating a provider should pay particular attention to the qualifications of the intrusion analysts. Many MSSPs tout the number of CISSPs at their organization. While the CISSP is respectable certification, it is not an operational-level certification and you should not give it much weight at this level. Instead, security teams should look for an MSSP's intrusion analyst team to possess a more practitioner-level certification, such as SANS' Global Information Assurance Certification (GIAC). In particular, intrusion analyst teams should specialize in the GIAC Intrusion Analyst track, which provides them with the tools they need to rapidly identify, analyze and respond to threats. Organizations should feel confident in their provider's ability if 100% of the MSSP's analysts carry a GIAC Intrusion Analyst certification.

At the management level, careful consideration needs to be paid to the team's vision of the company. From the top down, is the MSSP focused on delivering Managed Security Services or are they using services as a way to increase their product sales? This is very important because it determines whether the provider will have the breadth of experience necessary to perform in a best-of-breed environment or if they only have experience with their company's own products. Vision also plays an important role depending on your objectives. Many MSSPs have a general, managed anything

security vision. These providers are excellent for companies that do not have the capacity or inclination to handle security internally and are looking for a way to outsource the entire function. On the other end of the spectrum are providers that specialize in Threat Management and partner with internal security teams to enhance their organization's security posture. These providers focus their service offerings around providing the capabilities necessary to protect, detect and respond to threats before damage is done.

Process

The second category is the Managed Security Service Provider's processes. Processes facilitate the effective delivery of the provider's services. An important, but often neglected process is the ability to enable real-time service delivery visibility. An MSSP should adhere to an OPEN Service Delivery methodology. This methodology allows clients to see the status of their security and service delivery every second of every day. By adopting this methodology, the MSSP needs to have the proper processes in place to show clients real-time information through a portal. Many providers will only post incidents after they have been analyzed. By not presenting all security events, the client will not gain enterprise-wide security visibility and will never know the true level of threats facing their organization. Companies should seek providers that present them with all the events and their status in real-time via the client portal.

Availability of the monitoring infrastructure is obviously of critical importance. However, it is surprising how many providers do not have processes in place to detect failures in their own monitoring systems. Even fewer providers conduct trending and behavioral analyses to detect abnormal traffic patterns. Without conducting these types of analyses, a provider will not be able to catch a sudden drop-off in their security monitoring visibility. For example, when a client makes an improper switch configuration change on a network where an intrusion detection system resides, most providers will not be alerted to a sudden reduction in visibility. To them it would look like a mere slow-down in events. Only providers that conduct continuous analysis on behavioral patterns will realize that something is not right with the monitoring infrastructure. It is obviously very important to seek out providers who conduct this type of analysis to ensure service availability.

The MSSP should have processes in place to feed information from one service to the next, in order to accurately identify threats and respond to them immediately. With an integrated delivery platform, the MSSP's services will work together to protect client organizations. With integrated services, threat research teams are able to supply intrusion analysts with information about emerging threats. Analysts can then proactively update

signatures and increase vigilance over vulnerable client networks. Without integrated services, each team would operate as a silo of information, which causes service latency and increases the potential for threats to cause damage.

Technology

Technology is the foundation of a Managed Security Service Provider's ability to deliver quality service. Without the right technology solutions, it is difficult for the provider's analysts to properly investigate and respond to threats. One example is whether the MSSP decides to outsource core competencies by buying off-the-shelf solutions or to build these competencies in-house. Of particular importance is the security event monitoring platform and threat intelligence they use to deliver their services. If the platform they use was not developed in-house, then the provider is at the mercy of the vending software company. Over time, this will inhibit their ability to improve analysis and response times since they will not be able to make the changes necessary to manage the ever-increasing amounts of security events. The bottom line is that by using off-the-shelf solutions for their underlying platform, a provider's ability to innovate, scale and deliver an exceptional service will be outside of their control. Organizations should consider using providers that have developed their core service foundations in-house to ensure they receive a high level of service over time.

Having an in-house team of researchers delivering threat intelligence is important because it improves the time it takes to deliver advanced warnings to emerging threats. Additionally, having an in-house team further protects an organization by enabling the intrusion analysts to use this valuable information to proactively update signatures and take other measures against the impending threat. Organizations will attain a higher-level of service from a provider that focuses on MSS and has developed the necessary infrastructure in-house.

An important element of effective security monitoring is the ability to examine the packet decode from a network intrusion detection system. The packet decode provides you with the raw packet information. With this information, a skilled analyst will be able to analyze the packet to reduce the likelihood of a false positive. Most MSSPs only look at an event as it is recorded in an SNMP trap or syslog. This hinders their ability for thorough examination and may result in unnecessary calls to their customers. MSSPs that can collect the packet decode with the actual event in real-time and deliver this information to the analysts in a single integrated view will demonstrate a consistently higher level of accuracy in their analysis of a threat. Organizations should seek out providers that form tight relationships with network intrusion detection providers to attain and integrate real-time packet decodes from the events they produce.

Another critical analysis component is having technology capable of analyzing all events from monitored devices in real-time. This should seem basic, but unfortunately, many providers are not able to perform this function. Usually this is due to their inability to correlate real-time intrusion detection alerts with events generated by the firewall, which are sent to the SOC periodically. Without having all events aggregated in real-time, the correlation capabilities are greatly reduced, resulting in more false-positives and negatives. By finding a provider that is capable of analyzing all events in real-time, an organization will attain a higher level of service.

One of the most important components of a provider's technology is the way they set up their event filters. These filters should be behavior-based to separate known bad, from known benign and keep all anomalous events for further analysis. Again, this sounds basic, but many MSSPs examine only known bad events in real-time and analyze the anomalous

events at their leisure. However, typically most new threats are discovered from the unknown events. MSSPs that do not analyze both known and unknown events in real-time will not perform well for their clients.

The last technology consideration is the monitoring platform's architecture. MSSPs that use site to SOC VPN connections will not be able to fail over seamlessly to redundant facilities when emergencies arise. The reason for this is the configuration changes that must be made to the VPN at a client's site. The result is minutes, if not hours of service unavailability. Organizations concerned with requiring their provider to have robust disaster recovery plans should ensure that the provider they choose does not require VPN connections to the SOC.

Conclusion

In summary, there are 11 elements necessary to ensure a successful partnership with a Managed Security Service Provider. These 11 elements can be grouped under the categories of People, Process and Technology. They include:

People


- ▲ Intrusion Analyst team should hold a SANS' Global Information Assurance Certification (GIAC)
- ▲ Management-level focus on Managed Security Services with no product conflict of interest

Process

- ▲ The Managed Security Service Provider should adhere to an OPEN Service Delivery methodology
- ▲ The SOC must have processes to monitor the monitoring infrastructure through trending and baselines
- ▲ There must be processes in place that integrate information from one service into all other services

Technology

- ▲ The provider must have built their security event monitoring platform from the ground up
- ▲ Security intelligence capabilities, including the research group, must be in-house
- ▲ Monitoring platform must gather granular event information, such as the packet decode from IDS events
- ▲ The security event monitoring platform must be able to gather events from ALL devices in real-time
- ▲ The monitoring platform's filters must look for both known and unknown events in real-time
- ▲ The Provider's platform must not require site-to-SOC VPN connections as fail over will be hampered in emergencies

With many Managed Security Service Providers to choose from, organizations need to conduct careful evaluations to find the right partner for them. An MSSP should have strong people, processes and technologies in place to ensure that the provider delivers the highest level of service available. This article has highlighted a few important points that organizations should take into consideration when they perform their evaluation. By using them as a guide, they will increase their chances of finding the best Managed Security Service Provider for their needs. 

Steven Drew is Chief Operating Officer at LURHQ, a Chicago-based Managed Security Services Provider. Steven joined LURHQ in December 1999 with responsibility for leading LURHQ's Intrusion Analysis team and the delivery of LURHQ's Managed Security Services. In this role, Steven has been responsible for analyzing millions of potential threats to ensure LURHQ's clients are continuously protected from malicious activity. Steven started his career at Horry Telephone Cooperative (HTC) where he was responsible for developing HTC's Network Operations Center and the roll out of several service offerings, including Integrated Services Digital Network, Internet Service Provider and Asynchronous Transfer Mode data services. Steven has authored numerous articles on Threat Management, and has appeared as a guest commentator on information security news stories twice on MSNBC. Steven is a GIAC Certified Intrusion Analyst. In addition, he holds a BS in Computer Engineering from Clemson University and an MBA from Winthrop University.

