Clearwater

5 Time-Saving Tips for Evaluating a Managed Security Provider

Support the Unique Needs of Physician Practice Groups

Evaluating a Managed Security Provider

A good Managed Security Service Provider (MSSP) can quickly provide highly detailed security operations and insight for your business. This goes beyond being able to manage your firewall and endpoint security alerts. Too often multiple alerts are determined to be false positives leaving you wondering how this is helping the security posture of your organization. The goal was to optimize resources to avoid wasting time and manage cyber risk better. With all that it takes for a medical group to grow equity and expand healthcare services across multiple locations and regions, do you have the time to manage you rmanaged security provider?

Providing 24x7 security operations (SOC) is about constantly investigating and assessing security warnings and evaluating cyber risk. Providing service level agreements (SLAs) is expected, but having alerts passed to you with minimal investigation is what may occur. Not all managed security provider models are the same, nor are the outcomes. Clearwater is here to help you avoid any misunderstanding and give you what you need to know so you can select the right Managed Security Provider for your needs, and one that is focused on the specific risks of healthcare providers.

> Managed SOC services may not be the best way to fulfill your security needs. ***As one type of managed security provider these organizations take on the management of your existing security tech stack, offering 24x7 monitoring. They don't provide the technology or consult on best security controls. Coverage gaps in this model mean it can easily fail to protect healthcare data and make it difficult to conduct investigations with full contexual awareness - delaying the detection of threat actors at work.***

Validate your MSSP by asking about the following details in this document. Find out what kind of reporting transparency clients have regarding the number and quantity of incidents occurring across their environments. Confirm that your security service provider is able to support hybrid environments from corporate systems to specialized healthcare cloud environments. Healthcare providers, regardless of their size, are constant targets for threat actors. Optimizing threat detection and fulfilling compliance obligations by selecting a provider that deeply understands these requirements and can react quickly to the changing security and compliance landscape will ultimately save you precious time. Clearwater experts in healthcare, security, compliance and cyber resiliency provide this information so you can make the best decisions and achieve your goals.

Helpful Tips to Review when Evaluating an MSSP

There are over 10,000 MSSPs with various security offerings and specialities. Because service levels and expertise vary, being able to weed out those that won't fit your business goals is necessary. But if your're not an expert yourself, what areas should you look at when evaluating? We've put together this paper to push past the hype and save precious time in this endeavor. Find the right security provider to protect your business, and one you can trust to support your security and compliance goals. Here are the five tips:

Tip #1

They're Focused on Active Threat Detection and Hunting

Security engineers need to read every alert and uncover the story the alert is designed to tell, and ask the following questions. By assessing these items, security operations will know how best to pivot and investigate further:

- What is the intent of the alert and what is it meant to detect
- What are examples when this alert found malicious activity
- Where in the attack lifecycle does this alert live, signaling the severity of the situation

Just implementing endpoint detection and response (EDR) technology and relying on vendor dashboard functions is not managing your security. Security providers should leverage the best technology in providing the security services along with security operations expertise. This should include a monthly review of SLA on services along with the ability to address how the service meets the needs of your security compliance requirements.

> Managed Extended Detection and Response (XDR) ***is a popular topic, but only large organizations have the budget and resources to implement. Smaller organizations can enhance their security by leveraging MSSPs that have XDR platforms with Security Orchestration and Response (SOAR), optimizing the threat investigation across a variety of customer data sources and threat intelligence.***

Tip #2

They Conduct Enhanced Investigations without Asking

This is where the experience of security engineers, not in years but in threat exposure experience, makes a difference. SOC engineers that have oversight of a wide variety of companies and environments scale faster than in-house security analysts.

Knowing what to do next and the speed in which they can threat hunt requires access to additional data sources that must be readily available and easy to assess:

- Logs from associated systems and firewalls
- Research and known indicators of attack based and their context
- Vulnerability exposure across the environment(s) based on patch status

While this may sound straightforward, for many organizations doing this themselves, this means remote access to the various sources of logs and systems that takes up precious time. This gives the threat actor more time to map his or her maneuvers. Keeping a low profile and staying under the radar is the trade secret for those trying to compromise your business. Architecting security for maximum efficiency is not an easy task; security providers that offer more than just endpoint MDR should be able to provide log and firewall security management. For the protection of your environments (hybrid and cloud), this gives them the sources of data to enhance their investigations quickly.

Tip #3

They Dig Deep to Understand Prevalence and Persistence

Alert storms are common in security, with too many systems and too many logs with overly high verbosity settings. It is all too common to have reoccurring alerts, and it's even worse when they are ignored because the last investigated revealed it was a false positive. However, a managed detection and response provider's job is to understand this prevalence and hone in on why it these alerts continue to occur.

Your security provider should be asking questions like:

- How often does this alert fire?
- Does it happen across connected networks, accounts, or hosts?
- Did this alert lead to evidence of unauthorized activity or lateral movement?

As security technologies go deeper into behavioral analysis, the number of potential alerts has also increased. Those trying to do this themselves find the maintenance and overhead of these advanced systems too costly. This tedious aspect of security operations is necessary for all sizes of business, but only a few have the bench depth or patience for this activity when other higher-order tasks are asked of security operations. Ideally, the best MSSPs will proactively discuss these situations and consult on how best to optimize the signal-to-noise ratio for the highest outcomes with their clients.

Tip #4

They Know the Value of Obtaining Context from All Angles

This continues to be a sticking point when it comes to managing security, it is all about the context of type of alert and when an alert occurs. This goes beyond monitoring networks and endpoints, but it must consider business context as well. For example, if it was determined a scan was triggered, did it come from a known and approved scanning source?

Alerts cannot be handled as singular events. Security operations analysts and engineers are not factory line workers, but need to investigate the relationships of how events unfold and are inter-connected with other sightings. Bringing together threat intelligence, evidence, and historical context is the best way to get the macro security climate, the immediate situational aspect, and determine what occurred in the past to help evaluate and triage.

Without having this information readily available, any provider is at a handicap. Consider how security providers gain context from all angles by asking:

- Is historical data and alerts kept without penalizing clients with storage or data fees?
- Are there details against escalated events describing the root cause and disposition?
- Do you have access to this information and the historical trends across your environments?

Tip #5

They Provide Incident Response and Orchestration at Scale

The ideal situation is to have no escalated incidents, and a strong security posture. But if a security incident were to occur, would you know exactly what your managed security provider would do? Incident response to active threats is critical to minimize risk and contain the potential damage an intruder could cause. Small to medium sized enterprises are compromised as much as larger organizations, yet they have smaller budgets to address the issue. Support during a critical incident should be about teaming with a secuirty provider that you trust and looking for these key attributes:

- The option to individualize escalation plans based on your business
- Continuous updates and video calls with the leaders providing active oversight of the situation
- Dashboard access to the open tickets and triage actions occurring

Not only do top-tier security and threat hunters actively engage during incident response, but good managed security providers look out for the security and well-being of their clients. While managed security service providers cannot manage everything, they can provide guidance on additional recommended actions a company should initiate based on the variant and nature of the attack. This might include forcing password reset for admins, enforcing two-factor authentication (2FA), and isolating system backups. Having an active partner and expert to advise and reccommend next-best actions to coodinate against active threat tactics is what you need when you chose an MSSP.

The Next Steps to Finding the Right MSSP

There are many types and models of managed security service providers. Clearwater focuses on providing the security foundation for healthcare providers of all sizes. Our security operations center (SOC) services run 24x7 with active staff round the clock responding to and investigating security events. We make advanced security accessible through our proprietary platform and industry-leading technology partners to orchestrate the management and correlation of security data. However, it is our service and support that win over clients year after year as we take on their security and compliance challenges. Learn more about our Managed Security Services:

24x7 Threat Detection & Response (Hybrid & Cloud Support)

- Security Device and Firewall Management
- Managed Endpoint Security Management (MDR)
- Log Management
- Incident Management
- Vulnerability Management

Corporate Working Environments and Security Management (Microsoft)

- Managed Microsoft 365
- Managed Intra ID (formerly Active Directory)
- Managed Azure Virtual Desktop (AVD)

Clearwater helps organizations across the healthcare ecosystem move to a more secure, compliant, and resilient state so they can achieve their mission. The company provides a deep pool of experts across a broad range of cybersecurity, privacy, and compliance domains, purpose-built software that enables efficient identification and management of cybersecurity and compliance risks, and a tech-enabled, 24x7x365 Security Operations Center with managed threat detection and response capabilities..

Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact