5 Tips for Evaluating an MSSP to Save you Time

Details for growing organizations to evaluate security service providers that will improve cybersecurity outcomes

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 if you could do it better in-house.

Providing 24/7/365 security operations (SOC) is about constantly investigating and assessing security warnings and evaluating cyber risk. Providing service level agreements (SLAs) is expected, but passing on alerts with minimal investigation is what may occur.

Validate your MSSP by asking the following details and find out what kind of reporting transparency clients have regarding the number and quantity of incidents occurring across their environments.

1. Exceptional Detection and Methodology

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, the SOC 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. Providers should leverage the best of technology to provide the security services along with the security operations expertise. This should include monthly review of SLA on services along with the ability to address how the service meets the needs of your security compliance requirements.

SOC services are limited as they manage existing security solutions and don't provide the technology or control how alerts are configured.

continued on next page ›

2. They Can Provide Enhanced Investigations

This is where the experience of the 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 in this aspect than in-house security analysts.

Guidance on 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:

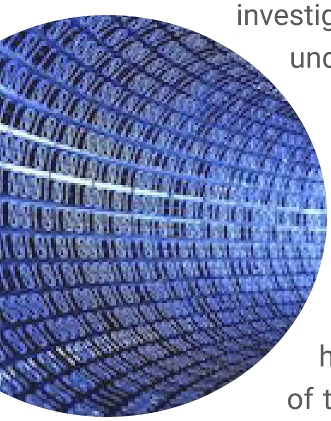
Obtain logs from associated systems and firewalls
Research and correlate with indicators of attack based on threat context

While this may sound straightforward, for many organizations this means remote accessing to the sources of logs and systems giving 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, when providers can expand beyond just MDR and provide log and firewall security management they can easily enhance their investigations quickly.

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

3. Dig Deep to Understand Prevalence

Alert storms are common in security, too many systems, too many logs with overly high verbosity settings. It is all too common to have reoccurring alerts and even worse when they get ignored because the last time it was investigated 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.



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 something that 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 MSSP companies will proactively discuss these situations and consult on how best to optimize the signal-to-noise ratio for the highest outcomes with their clients.

continued on next page

4. Confirms Context from All Angles

This continues to be a sticking point when it comes to managing security, it is all about the context of what and when an alert occurs. This goes beyond just monitoring networks and endpoints, but it must bring in the 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. SOC engineers are not factory line workers, but investigators into 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 what occurred in the past to help evaluate and triage.

Without having these items readily available any provider is at a handicap. Consider how providers achieve the ability to have context from all angles:

Is historical data and alerts kept without penalizing clients with data feed charges or storage capacity limits?
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?

5. Optimizes Incident Response and Orchestration

The ideal situation is to have no escalated incidents. But, if one 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 much more to lose, and smaller budgets to address the issue. Support during a critical incident should be about teaming with a provider that you trust, and looking for these key attributes:

Are there options to individualized escalation plans based on your business?
Will you receive continuous updates and video calls with the leaders providing active oversight of the situation?
Do you have 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 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 2FA, and isolating system backups.

continued on next page ›

Finding the Right Managed Security Service Provider

There are many acronyms for the diverse types and models of managed security service providers. TECH LOCK bundles endpoint detection and response (EDR) technology, firewall management with log and threat detection. Our security operations center (SOC) services runs 24/7/365 with active staff round the clock responding to and investigating security events. With a focus on managed detection and response (MDR), the incorporation of firewall management and log services extends these services (XDR) with security telemetry from multiple perspectives allowing us to optimize security for small to medium-sized enterprises. 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.

DETECT AND RESPOND

Security Device and Firewall Management
Endpoint Security Management
Log Management
Incident Management
Vulnerability Management

COMPLIANCE MANAGEMENT

Bundled Compliance Certification
Compliance Maintenance
Compliance Gap Analysis

VALIDATION

Cybersecurity Assessments
Penetration Testing
Third-party Risk Assessments
Compliance Certifications: PCI DSS, HITRUST, FISMA, ISO, NIST, PRIVACY, SOC

TECH LOCK®

320 E. Big Beaver Rd, Suite 145 • Troy, MI 48083

info@techlockinc.com

847.245.3727

www.techlockinc.com

TECH LOCK enables organizations to navigate, detect and respond to today’s modern cybersecurity and compliance challenges. We provide 24/7/265 threat detection and incident response accessible and affordable. TECH LOCK’s full spectrum security-centric approach delivers value to our clients through defined and measurable outcomes combined with independent cyber research, specialized skills and premium customer support and service.