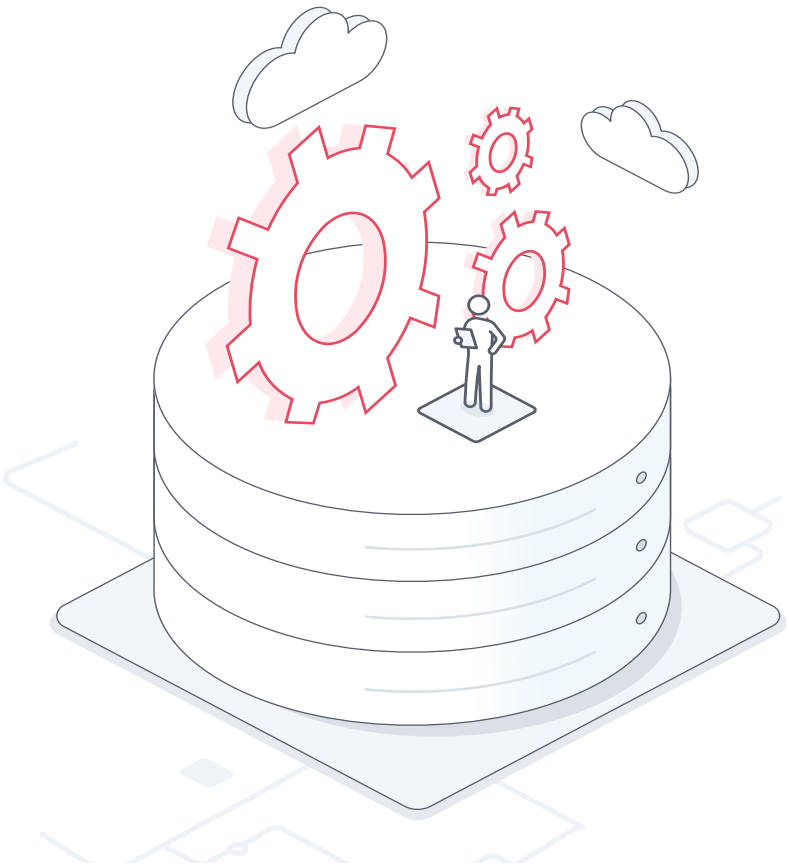
5 Time Saving Tips for Evaluating a Managed Security Provider

Supporting CMMC Needs for the Defense Industrial Base (DIB)

Redspin®
A Division of Clearwater

Contents



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 if you could do it better in-house. With all that comes with CMMC readiness and eventual certification, do you have the time to manage your managed 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. Redspin 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 aligns to your CMMC goals.

> **Managed SOC services alone may not fulfill your CUI 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. This can model can easily fail at protecting CUI due to existing coverage gaps across the environment, and lack the ability to investigate with full contextual awarreness.

Validate your MSSP by asking the following details we'll share 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 gov't. cloud environments. As Department of Defense (DoD) vendors look to optimize the way they can protect CUI data selecting a provider that can fit these requirements and can accomodate the changing security and compliance goals for CMMC will ultimatley save you precious time. Redpin understands the crucial role that DIB contractors play in supporting the DoD and our Warfighters and wants to ensure the health of your business to continue to serve this mission.

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 varies, being able to weed out those that won't fit your business goals is necessary. But if your not an expert yourself what areas should you look at when evaluating? We've put together this paper to dig into that problem and give everyone the opportunity to push past the hype and save precious time in this endeavor. Find the right security provider to protect your business on your behalf, and one you can trust to support your security and compliance goals. Here are 5 tips to use when evaluating an MSSP:

The Provider is 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. 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.

> **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.

Delivers Enhanced Investigations without Asking

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 doing this themselves this means remote access to the various sources of logs and systems taking 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 (hybird and cloud) this gives them the sources of data to enhance their investigations quickly.

They Dig Deep to Understand Prevalence and Persistence

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 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.

Knows 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 just monitoring networks and endpoints, but it must bring in business context as well. For example, if it was determined a scan was triggered did it come from a known and approved scanning source?

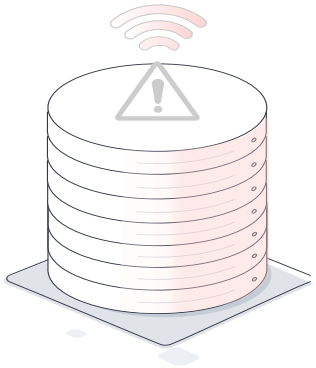
Alerts cannot be handled as singular events. Security opertions analysts and engineers are not factory line workers, but investigators into the relationships of how events unfold and are inter-connected with other sightings. Bringing together threat intelligence, evidence, and historical context is the 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 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**

Provides 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 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 the option 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. 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 acronyms for the diverse types and models of managed security service providers. Redspin, a Divison of Clearwater, focuses on providing the security foundation for DoD vendors of all sizes. Our security operations center (SOC) services runs 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**

Redspin, a division of Clearwater, has become one of the most trusted cybersecurity companies within the Cybersecurity Maturity Model Certification (CMMC) ecosystem. Our exclusive focus on tailoring our IT security assessments and consulting services for each client delivers peace of mind by lowering the risk of a security incident or breach and achieving compliance objectives.

Since our founding in 2001, we've performed thousands of security assessments, have become thought leaders in IT security and CMMC, and helped countless clients control their security risk, develop their compliance and security strategies, stay ahead of the competition, and avoid a breach headline.

Redspin is a leading provider of cybersecurity consulting using various frameworks including NIST CSF, CMMC, ISO 27001, HITRUST, and PCI DSS. We've helped many Fortune 500 and leading growth companies in highly regulated industries including government, aerospace, financial, technology, and manufacturing achieve their goals related to the CMMC initiative, and improve their cyber readiness + resiliency through a strategic and proven approach to reduce cyber risks and safeguard sensitive information.

Have questions? Engage with Redspin for a specific discussion about your organization's approach.

Redspin.com/Contact