Selecting a Managed Detection and Response Service: What Clients Think and Prospects Want

AN ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) WHITE PAPER

Prepared for Secureworks

By Paula Musich

June 2020

Selecting a Managed Detection and Response Service: What Clients Think and Prospects Want

INTRODUCTION

Organizations large and not so large are waking up to the need to find expert help in managing the process of hunting down and remediating threats within their IT infrastructure. As threats continue to evolve, IT security practitioners accept that their networks and infrastructure have already been compromised. It is critical now to find those threats and shut them down before they do serious damage. The IT security skills gap has contributed to the need for more threat hunting expertise than many organizations can muster.

This has fueled great interest in managed detection and response (MDR) services. The new EMA research report, "Managed Detection and Response: Selective Outsourcing for Understaffed SOCs and the Platforms That Enable MDR Services" revealed that among those not already using an MDR service, only 6% of the IT professionals surveyed said their organizations were not looking for MDR services. Such demand has created a gold rush mentality among a rapidly expanding base of startups and established managed security services providers hustling to offer MDR services. How do prospective MDR clients determine which of those providers represents the right fit for their own unique requirements?

Based on the findings of the research report published in May 2020, here are five tips to consider in selecting an MDR provider.

TIP 1: FLEXIBILITY IS KEY

How extensive is the MDR provider's coverage, and how well does that map to your organization's environment? Does the MDR provider just focus on endpoints? The network? What about your cloud workloads? There are MDR providers of various stripes, and each provider comes at the problem from a certain perspective. Some may just outsource management of a SIEM. Others may be focused solely on endpoint detection and response (EDR). Others may focus on network detection and response (NDR). Flexibility is key, and there are several dimensions to it. The EMA research on MDR usage and demand conducted in early 2020 found that the most commonly monitored elements for organizations using an MDR service include IoT devices, cloud workloads, networks, and servers. Still, a small percentage of MDR users also had their service provider monitor containers and mobile endpoints. EMA also found that when it comes to selecting an MDR provider, a clear majority of current users of MDR services rated coverage of cloud workloads as well as industrial IoT or other IoT devices as very important in their selection criteria.

TIP 2: MIND THE (SKILLS) GAPS

It's important to look at the depth of expertise that will be applied to your organization, assess the skills your organization already has in existing personnel, and seek to complement those with skills the MDR provider can bring that fill in gaps for your organization. It's not unreasonable to ask for the qualifications of the security analysts or threat hunters that support clients from the MDR provider's SOC. Having a conversation with your prospective MDR provider's analysts will be helpful in assessing their level of skill, experience, and training, and in determining whether there is a good fit for your organization's requirements. Ask to see the types of reports that they produce for clients and ask them about different scenarios your security team has either encountered or anticipates to see how they would respond. Do their answers make sense to your security team? Do they adequately address your concerns? Do they demonstrate a willingness to customize the MDR service to your specific requirements, or do they appear to take a cookie-cutter approach that is applied to all clients?

TIP 3: YOUR TOOLS OR MY TOOLS?

Many organizations invested heavily in different threat management technologies over time to keep abreast of the changing threat tactics and techniques. A subset of those organizations found such tools too complex, or they found their internal teams not up to the task of putting those tools to their most effective use. This is especially true for midmarket organizations with fewer than 1,000 employees and even small to medium-sized enterprises with 1,000 to just under 5,000 employees. EMA's research found, for example, that among those organizations interested in acquiring an MDR service, approximately two-thirds of SMEs expressed an interest in both managed SIEM and EDR services.

For such organizations, it may not make sense to select an MDR provider who relies on their own monitoring technologies. The need to install an outside MDR provider's sensors or other monitoring gear to onboard the service could extend the time it takes to operationalize the service to weeks or even months. At the same time, there is no guarantee that the MDR provider's own monitoring technology won't introduce incompatibilities that make the onboarding process even more complex and time-consuming. Finally, your organization may not want to obsolete the significant investment it's already made in SIEM, EDR, or other detection and response technology. While most pure-play MDR service providers often use their own monitoring technologies, managed security services providers (MSSPs) are better prepared to work with a variety of existing monitoring technologies already in place.

TIP 4: CAREFULLY WEIGH COST VS. COVERAGE TRADEOFFS

Another consideration prospective MDR services buyers should weigh before selecting a provider is how much coverage (timewise) your organization requires. Is your organization just looking for coverage during non-business hours, 24x7x365, or somewhere in between? In its research, EMA found that the answer often depends on the size of the organization. For large enterprises with 5,000 or more employees, 75% of MDR users contract for 24x7x365 coverage, while just over half of respondents at organizations with between 1,000 to 4,999 employees opt for 24x7 coverage minus holidays. Full coverage comes with a bigger price tag that smaller organizations are often not able to swallow. One other note: for a solid majority of MDR services users, contracting for such services is seen as augmenting that capability rather than replacing it entirely. That was true for 67% of MDR respondents in the survey.

TIP 5: PLAN FOR THE FUTURE

In the MDR research project, EMA found satisfaction levels among users of those services to be relatively high. When rating their overall MDR service level, just over half of all respondents using an MDR service said they were extremely satisfied. Fifty-six percent of those MDR users were extremely satisfied with the level of expertise available to them. Just under half said they were extremely satisfied with the availability of the service providers' professionals. Given these good marks, it's no surprise that those working with MDR providers are thinking about adding on additional services from those providers. Given that the IT security skills gap isn't going away anytime soon and the desire to get the most out of the much more robust information security budgets in place today, determining what other security functions your organization will want to outsource in the future is another important criteria in the selection process. Can the MDR providers you're evaluating take on the additional work your organization may want to outsource in the future? More often than not, MDR users—especially those happy with the services they contract for—also look to those same providers for help with other security tasks related to maintaining good security hygiene, assessing risk, and more. The EMA MDR research project asked respondents to indicate which, if any, of six different security functions they wanted from their MDR providers that were not available to them. Topping the list at 17% each were penetration testing and risk assessment, followed by risk reporting, automation playbook recommendations, and vulnerability remediation at 16% each. It was interesting to note that only 4% of the MDR users indicated none of the above. Whether those functions are viewed as important but less strategic, or whether they represent holes not easily filled internally for the existing security program, it's important to find an MDR provider that can step in and help with other pressing needs.

A FEW FINAL THOUGHTS

There are multiple dimensions involved in onboarding an MDR service that demand some upfront planning before selecting an MDR services provider. In no special order, those include the following questions: How quickly can they onboard your organization and start hunting threats? What do the reports they provide to clients include, and do they make sense for your business? What metrics will they give you to show how effective they are? Do they do remediation themselves, or do they just confirm a security event is an actual attack and hand remediation back to your team?

It's critical to do your homework before starting your journey to evaluate whether an MDR service is the right choice for your organization, and which providers best suit your organization's needs. Clearly establishing requirements before evaluating providers is a good first step on the path to MDR service adoption.

ABOUT SECUREWORKS

Secureworks® (NASDAQ: SCWX) is a technology-driven cybersecurity leader that protects organizations in the digitally connected world. Built on proprietary technologies and world-class threat intelligence, the company's applications and solutions help prevent, detect, and respond to cyber threats. Red Cloak™ software brings advanced threat analytics to thousands of customers, and the Secureworks Counter Threat Platform™ processes over 300B threat events per day. More than 4,000 customers across over 50 countries are protected by Secureworks and are collectively smarter. Exponentially Safer.™

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates® (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
www.enterprisemanagement.com

3984.06032020