What's Fueling Exploding Interest in Managed Detection and Response Services?

AN ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) WHITE PAPER

Prepared for Secureworks

By Paula Musich

June 2020

INTRODUCTION

Visions of a largescale SOC—fully staffed with dozens of threat hunters quietly and efficiently investigating a well-organized and correlated set of events—dance in the heads of many CISOs. The reality for most IT and IT security executives is far from that vision, however. For most, it looks a lot more like a war zone: chaotic, disorganized, and staffed by a less than optimal number of security professionals tasked not only with threat hunting, but a variety of other security-related functions. Despite the desire to move beyond firefighting mode to address more strategic goals, many remain mired in managing too many IT security tools, handling an unmanageable volume of alerts populated by way too many false positives, and battling the blazes of breaches caused by increasingly sophisticated attacks that breeze past existing defenses.

Given this uncomfortable reality, it's no surprise that interest in managed detection and response services has never been greater than it is today. In an Enterprise Management Associates research report published in April 2020, only 6% of organizations that aren't already using an MDR service are not thinking about it, according to the IT and IT security respondents who took the survey in early 2020. The report, titled "Managed Detection and Response: Selective Outsourcing for Understaffed SOCs and the Platforms that Enable MDR Services" found that nearly three-quarters of the 179 respondents were not yet using an MDR service, but among those non-users, 46% indicated their organizations were currently evaluating an MDR service. Another 33% said their organizations were considering adopting an MDR service and another 15% said their organizations were planning to evaluate MDR services in the next 12 to 18 months. Interest is especially keen among midmarket organizations, defined as having between 500 and 1,000 employees. Sixty-seven percent of those respondents said their organizations were currently evaluating MDR services.

TOP-LEVEL ISSUES: A PERFECT STORM

Fueling such heightened interest in MDR services is a perfect storm of factors that have converged in the last few years to make the job of protecting an organization's digitized assets harder than it's ever been. The process of detecting and responding to threats has become extremely difficult, thanks to an attack surface that has grown exponentially with cloud adoption, the growing deployment of IoT devices in enterprise and operational networks, and most recently with the huge number of employees now working from home, using their home networks shared with the rest of the family to access critical company data and conduct business online. That's coupled with a significant rise in the number and sophistication of threats from a well-organized ecosystem of threat actors who share tools, tactics, techniques, and information more readily and efficiently than defenders.

Then, of course, there is the IT security skills gap, which isn't going away anytime soon. Estimates of the size of the gap vary according to different sources. On the lower end of projections, the Center for Cyber Safety and Education projects that 1.8 million cybersecurity jobs will go unfilled by 2022.[1] On the higher end of the scale, Cybersecurity Ventures estimates that 3.5 million cybersecurity jobs will remain open by next year.[2] ISACA, the international IT governance association, reported in its 2020 State of Cybersecurity research that 62% of its respondent members said their organization's cybersecurity team is understaffed, and 57% reported having unfilled jobs on those teams.[3]

TOO MANY TOOLS IN THE CYBERSECURITY TOOLBOX

Beyond these top-level issues, other motivations are spurring more organizations to investigate MDR services. In EMA's survey, 41% of all respondents whose organizations were interested in MDR services indicated that their security teams were overwhelmed by the number of security layers or tools they had to manage. For too many years, organizations kept throwing more technology at the problem of keeping abreast of the growing number of threats. However, that begs the question: How many is too many? Palo Alto Networks' Matt Chiodi, chief security officer of public cloud, threw out a few numbers in an RSA 2019 presentation. He said small organizations average using between 15 to 20 cybersecurity tools, medium-sized organizations use between 50 to 60 tools, and large enterprises use over 130 cybersecurity tools.

The EMA research uncovered other, more subtle drivers behind the growing interest in MDR services. For example, 34% of organizations interested in MDR services expressed a desire to free up in-house security experts to focus on more strategic activities, 32% of those respondents indicated their organizations were looking to cut the cost of their security operations, and 29% said their organizations recently experienced a breach and could not respond adequately using existing personnel and technology.

LOTS OF CHOICES, BUT WHO CAN YOU TRUST?

The growing interest in MDR services has not gone unnoticed, and a quickly expanding field of competitors entered the market over the last few years. They range from small startups to large security vendors, such as Cisco, which recently entered the market with its own MDR service. Providers range from pure-play MDR services groups to managed security services providers that have added MDR services to their portfolios. This gold rush mentality makes it tough for prospective users of MDR services to identify the provider with the best fit for their requirements.

1 https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage
2 https://cybersecurityventures.com/jobs-05-30-2017/
3 https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2020/isacas-cybersecurity-study-reveals-struggles-with-hiring-and-retention-persist-more

MDR providers that can keep up with the increasing demand for MDR services while rising to the challenge of staying on top of emerging threats have some commonalities. Chief among those is a solid platform for their services that can quickly scale with demand and easily integrate with the customer's environment. Multi-tenancy is key for privacy, and automation that enables faster detection and response is a must. Also important is the effective use of threat intelligence and machine learning to speed detection of unknown threats. EMA found in its research that MDR users understand this, and the importance of the provider's platform as a selection criterion is critical. Just over half of respondents whose organizations were already using an MDR service gave the importance of their provider's underlying tools and technology in their selection process a 1 on a scale of 1 to 5, with 1 being most important.

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 and 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

4000.06242020