White Paper

Threat Intelligence Required for Effective Managed Detection and Response

Understanding the Underpinning of Threat Intelligence in MDR Solutions

By Christina Richmond, Principal Analyst

November 2019

This ESG White Paper was commissioned by Bitdefender and is distributed under license from ESG.

Contents

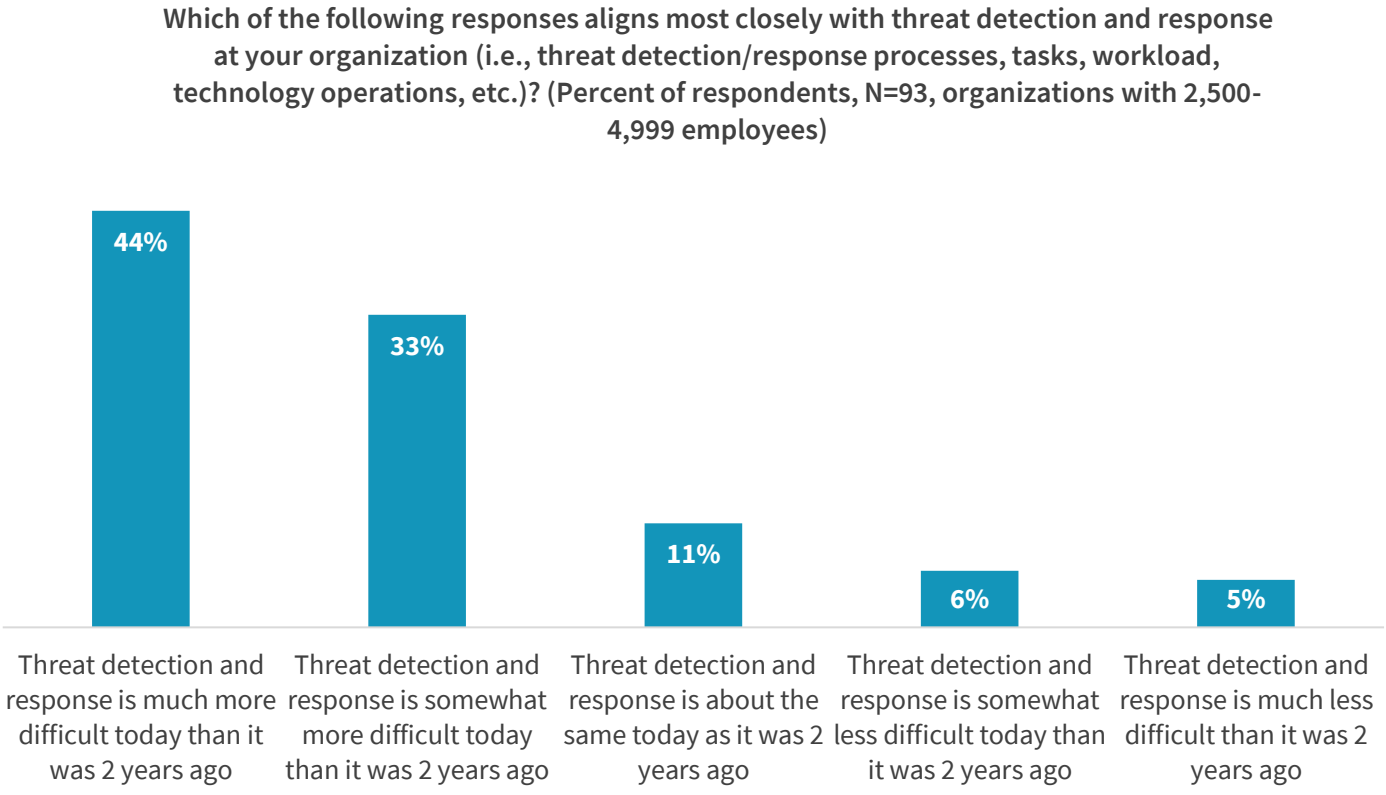
Executive Summary – Market Challenges

The State of Threat Detection and Response (TDR) Today

Cybersecurity professionals are responsible for threat prevention, detection, and response and most invest abundant resources, both human and budgetary, into security controls and processes in this area. However, these resources are constrained by the well-known cybersecurity skills shortage, which impacts every aspect of the security organization's remit. According to several multiyear studies conducted by ESG, the skills shortage continues unabated year-over-year. In 2019, 53% of respondents stated that the cybersecurity skills shortage continues to be problematic[1] and 74% of respondents to a separate ESG research survey stated that the shortage has had a somewhat to significant impact on the security teams that they've worked for over the past few years.[2] This shortage is a key issue that drives changes in how the security team prevents, detects, and responds to threats and drives an increased reliance on security services.

Threat prevention starts with good security tools hygiene and must-have controls like endpoint security software, intrusion prevention, and the like. However, despite all the controls in place, adversaries still break through threat defenses and compromise the environment. The rise to prominence of detection and response over mere protection capabilities is a direct result of security tool vulnerability to the continued rise in adversarial sophistication. The shift in focus to improved detection and response is due in part to the rise in credential abuse in modern day hacks.

Figure 1. Threat Detection and Response Is More Difficult at Midsized Enterprises Today than Two Years Ago



Source: Enterprise Strategy Group

[1] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey*, March 2019.
[2] Source: ESG/ISSA Research Report, *The Life and Times of Cybersecurity Professionals 2018*, May 2019.

Today, security professionals must go beyond signature-based blocking of adversaries and white-listing of good entities. They must also gather, curate, contextualize, and analyze vast amounts of internal and external threat telemetry. They must then correlate said data with known and unknown suspicious behavior and investigate and remediate issues before they become major data breaches. In fact, according to recent ESG research, 77% of midsized enterprises (companies with 2,500-4,999 employees, for the purpose of this white paper) indicated that TDR is more difficult today than it was two years ago (see Figure 1).[3] In addition, 34% of respondents said that the primary reason for difficulty with TDR is an increased volume of threats. The combination of the skills shortage and the dramatic increase in volume and sophistication of threats creates a workload that is unsustainable for the best of security teams.

Enter Outcome-based Managed Security Services: Managed Detection and Response (MDR)

Managed security services (MSS), or the outsourcing of security functions, has long been a fast-growing market and it is seeing double-digit growth in five-year forecast periods. For midsized enterprise organizations, MSS has been helpful in part because smaller companies do not have large security teams, and regardless of size, all organizations struggle to find the right expertise. MSS solutions have historically only provided alerts for customers to respond to, rather than responding to the alerts themselves. This creates additional workload for the customer, who is already taxed with few resources. However, in recent years, MSS providers (MSSPs) have added MDR services, which are fast becoming a key part of the MSS market and growing rapidly. Some estimate that this market will reach over $1.65B globally by 2022.[4] Because TDR is overwhelming and difficult, more than half of the organizations ESG surveyed chose to outsource management to a third-party and nearly all are satisfied with the service they are receiving (see Figure 2).

MDR is a newer market that focuses specifically on reducing mean time to detect (MTTD) and mean time to respond (MTTR). In a separate study on security services overall, MDR was selected on par with MSS,[5] demonstrating MDR's significant move into the MSS market. In ESG's TDR survey, 33% of midsized enterprise respondents stated that the need for rapid TDR improvement was one of their primary reasons for selecting MDR.

Figure 2. MDR Satisfaction at Midsized Enterprises

Source: Enterprise Strategy Group

[3] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019. All other ESG research references and charts in this white paper have been taken from the master survey results set, unless otherwise indicated.

[4] Source: Markets and Markets Press Release, *Managed Detection and Response Market worth 1,658.0 Million USD by 2022*, November 2017.

[5] Source: ESG Research, *Cybersecurity Services Survey*, to be published.

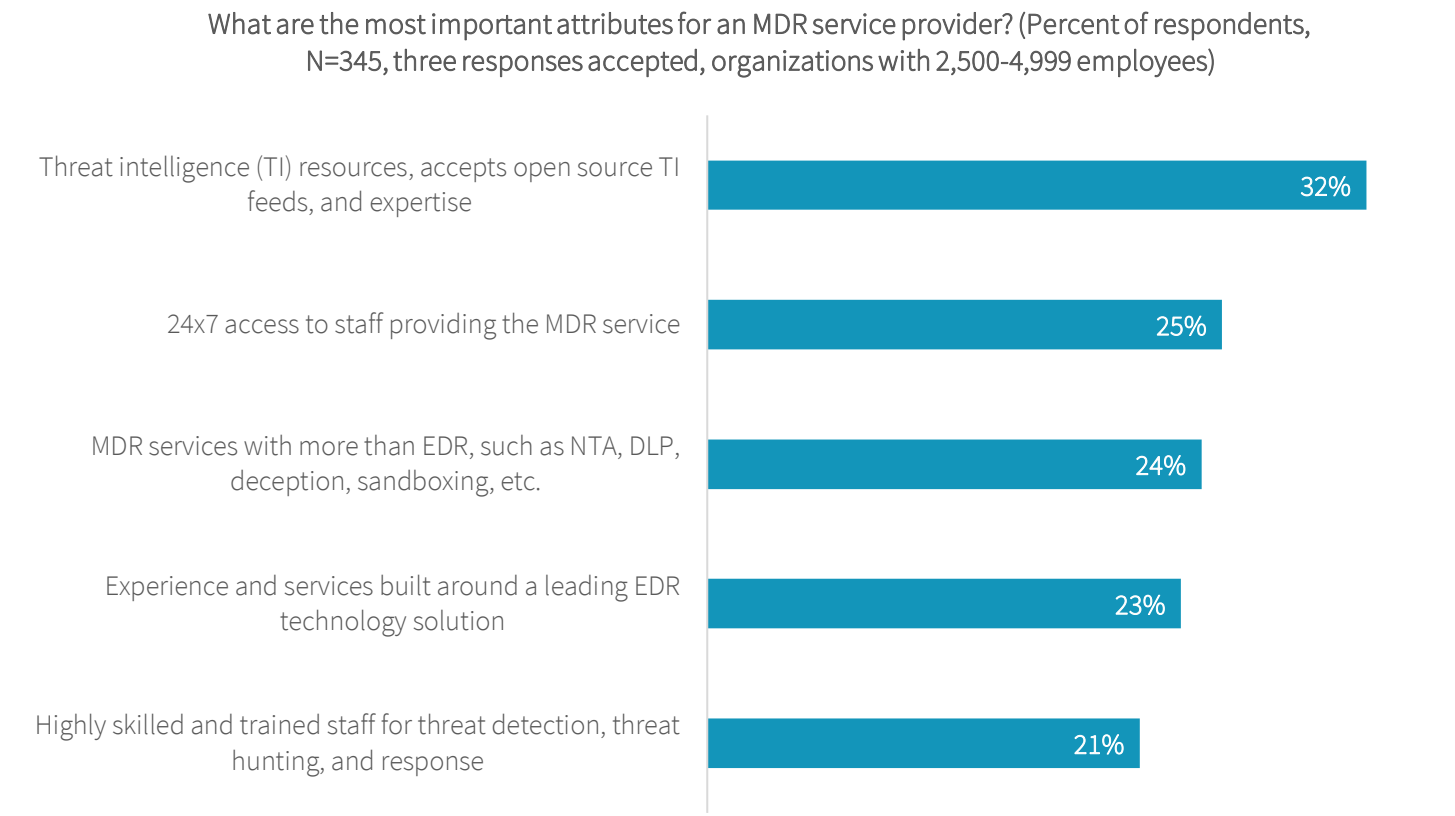
What Problems Does MDR Address?

Today's enterprise, regardless of size, is plagued with commodity malware, insider threats, and sophisticated yet often net-new human-based attacks. To combat these, it's not enough for organizations to layer prevention controls as they have done in the past. And it is imperative to detect and respond quickly to these threats so that the business can continue uninterrupted. Until recently, midsized enterprise organizations couldn't afford security information and event management (SIEM) tools or SIEM-based tools to parse millions of data logs across a distributed network and flag potential cyberthreats. They also couldn't afford to employ sophisticated analytics and dedicated teams or to build and operate security operations centers (SOC). MSS and outsourced SOC services helped reduce the cost of access to these tools and spread the monitoring and analysis resource load but also increased the need for personnel to respond to security alerts, many of which would be found to be false positives. MDR plugs the skills gap with threat hunters, researchers, and security engineers responsible for monitoring the customer network, analyzing alerts, *and responding* to real threats, once discovered, in addition to deploying technologies that detect modern day attacks at the endpoint and in the network. MDR employs either or both endpoint detection and response (EDR) and network traffic analysis (NTA) to detect attacks. Fifty-one percent of midsized enterprise respondents to ESG research preferred NTA. However, in recent years, EDR has become increasingly accepted; 26% of midsized enterprise respondents indicated that they use EDR and another 23% said that they use both EDR and NTA.

Threat Intelligence Tops the Attributes Required in MDR Solutions

The top attribute required for MDR solutions that was reported by midsized enterprises is threat intelligence. But also of importance is 24x7 access to staff (see Figure 3).

Figure 3. Top Five MDR Attributes Reported by Midsized Enterprises



Source: Enterprise Strategy Group

Two of the top five key attributes reported by midsized enterprises directly address the impact of the cybersecurity skills shortage. The first, however, points out the importance of threat intelligence telemetry. The term "threat intelligence" has lost all meaning with overuse. What is important is where this telemetry is sourced and how we augment and curate it with threat hunting. Threat intelligence feeds by themselves are comprised of simple indicators or artifacts pulled from a variety of sources: client data, global threat reports, threat attribution, indicators of compromise, etc. Most MDR providers source threat data from agents or sensors at the client endpoint and/or the network in addition to third-party subscription feeds. Threat hunting is an active cyber defense engagement and accretive to static data feeds. Cyber threat hunting is a labor-intensive, human-based "process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions."[6] In addition, some MDR providers also contextualize threat data to specific clients, by customer segment and industry. And, increasingly, threat data is mapped to adversary intent: what the adversary seeks, what part of the kill chain it is currently engaged in, what tactics, techniques, and procedures (TTPs) are being used, and so on. All of this makes threat data actionable and intelligent. Once we have actionable intelligence, it then matters how we employ it in MDR solutions.

Bitdefender's Solution Offloads Midsized Enterprise Staff Shortages and Outcome-based MDR

The Bitdefender Managed Detection and Response Service (MDR) is a managed threat-hunting and monitoring service for detecting and responding to intrusions and malicious activities using Bitdefender's suite of technology such as endpoint detection and response (EDR) and deep threat intelligence. It is focused on helping midsized enterprise customers with limited resources and technical skills to accurately protect complex, heterogeneous environments and respond effectively to evolving cyber threats.

All three levels of the Bitdefender MDR service—Bronze, Silver, and Gold—include endpoint detection and policy tuning and are based on Bitdefender's threat intelligence. Network traffic analytics and threat hunting are included at the top two tiers as is malware analysis. Silver and Gold service levels add greater customization to dashboards and preapproved response actions that Bitdefender will perform on the client's behalf such as resetting passwords, applying a patch, or isolating a machine. Bitdefender's researchers and analysts contextualize threat data, correlate it to specific customer industry and segment, and map potential breaches to the MITRE ATT&CK framework. In addition, the incident response time service level agreement (SLA) decreases from two hours at the Bronze level to one hour for Silver and 30 minutes for Gold. The service not only reduces the client's alert funnel, thereby alleviating staff burden, but responds quickly to resolve the problem before the attacker is able to move through the attack lifecycle. These actions, in addition to providing a suggested response action, help reduce the cybersecurity skills shortage impact and free up customer resources for the business.

The Bigger Truth

Today's cybersecurity challenges are many: a sophisticated adversary that continues to outsmart security teams, complexity of the security environment, and an overwhelming skills shortage. These issues are even greater for midsized enterprises, which are targeted no less by the adversary but have even fewer security resources. Companies of this size find TDR more difficult to perform today than it was two years ago, and they are outsourcing to MSSPs and MDR providers as part of the solution. Savvy security leaders in the midsized enterprise understand that they can't find internal threats and unknown or commodity malware with their limited budget and staff. They understand that threat data must be actionable and intelligent in order for them to make critical decisions, but they are unable to reduce the alert funnel because of resource challenges. MDR is a very appropriate service for the midsized enterprise organization to engage in

[6] Source: Wikipedia, *Cyber Threat Hunting*.

because it both reduces staff requirements and provides response to real-time potential incidents before they become harmful data breaches.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188