Bloor

Spotlight

Spotlight Paper by Bloor
Author **Fran Howarth**
Publish date **January 2020**

Managed detection and response services
...key to winning today's security battles

Managed detection and response services will help to bridge security gaps, providing access to advanced technology and skilled resources as and when needed to ensure that organisations can achieve their objectives.

Executive summary

Cybersecurity is reliant on a combination of people, processes and technology. Processes are essential for good governance, ensuring that business objectives can be met, risk is adequately managed, and that legal and regulatory requirements are fulfilled. Technology provides the means to ensure that those objectives can be met, and helps the organisation to protect itself from the harm caused by security threats and incidents. People are essential for the smooth operation of that technology.

But, as the threats that we face become ever more sophisticated and complex, the technology deployed to counter those threats has evolved rapidly to the point where it is similarly sophisticated and complex. Many organisations are struggling to make the best use of such technology, hampered by a lack of experienced staff to deploy the technology to its full potential. For many, managed detection and response services will help to bridge that gap, providing access to advanced technology and skilled resources as and when needed to ensure that organisations can achieve their objectives.

This document is intended for security and risk management leaders, and executive decision makers who are looking for the best way to improve their security posture and defeat determined adversaries. It describes how services can help to achieve security goals. A complementary document ***MDR market guide ...reducing the costs and risks of cybersecurity investments*** is available that describes the types of offerings available, features to look for and what best suits your organisation, referring to some of the leading players in this emerging market.

“Many organisations are struggling to make the best use of such technology, hampered by a lack of experienced staff to deploy the technology to its full potential.”

Introduction

Virtually every security executive these days laments the situation of facing too many threats, but of having too many disparate tools and not enough people to effectively deal with them. Threats are becoming ever more complex – as are the tools that have been developed to stop them. This is especially true given that it is an uphill struggle to protect networks from threats. It is now widely accepted that threat prevention cannot be guaranteed and the onus has shifted from prevention to detecting threats that have made their way onto the network, where they can cause real damage, and to finding a way to efficiently respond to incidents that have occurred.

The shift from products to services

These factors – escalating threats, complexity and a shortage of skilled security practitioners – is leading to a shift in the way that security defences are delivered. Technology vendors can no longer just deliver security products to organisations and let them get on with it, albeit with some level of professional help in terms of implementation and tuning, which can alternatively be provided by consultants. Over the past couple of years it has become apparent that organisations are looking for a much higher level of hands-on guidance to augment the capabilities of the security tools that they invest in.

According to Forrester, spending on cybersecurity services outpaced all other investments for the first time in 2018. Today, it estimates that four times more budget is being directed to cybersecurity services than anything else. Gartner estimates that spending on security services will account for 50% of cybersecurity budgets in 2020, estimating that $64.2 billion was spent on security services in 2019. This will not only continue, but rates of spending on security services will grow at rates in the double figures.

“Over the past couple of years it has become apparent that organisations are looking for a much higher level of hands-on guidance to augment the capabilities of the security tools that they invest in.”

The rise of managed detection and response (MDR) services

Given the challenges that they face, one area in which organisations are particularly looking for help is in detecting and responding to threats—hence, the burgeoning market for managed detection and response services. The 2019 cost of a data breach report from the Ponemon Institute estimates that the average time taken for an organisation to identify and contain a breach on their network is 279 days, which is 4.9% longer than the average for 2018. The longer it takes before a breach can be contained, the greater the potential for damage and the higher the total associated cost. Where the breach is the result of malicious or criminal activity, it takes even longer to identify and contain the threat at an average of 314 days, which adds to costs even further.

In recent research conducted by ESG, 82% of security professionals surveyed agreed that improving threat detection and response is a high priority, yet 76% state this is more difficult to achieve than it was just two years ago owing to the factors stated above. As a result, Gartner estimates that 25% of all organisations will be using MDR services by 2024, up from less than 5% in 2019. IDC estimates that take up is currently greatest among large organisations, finding that 41% of large organisations with more than 5,000 employees are looking to outsource advanced threat detection and response to third parties. However, it also sees an increasing opportunity for midmarket organisations to benefit from such services—especially those that have less mature security operations centres or that lack 24x7 staff coverage to manage complex detection tools. This is echoed by Garter, which estimates that 40% of midmarket organisations will choose MDR as the only managed security services that they use.

Why should you care?

The World Economic Forum polls private sector organisations worldwide annually to gauge what executives believe to be the greatest risks that they face. In the 2019 report, cyber attacks were cited as the second biggest risk that they face, coming behind only fiscal crises. In the 2018 poll, cyber attacks were seen as just the fifth biggest risk facing business, showing how big and fast growing the problem is becoming.

Digging deeper into the results, cyber attacks are seen in 2019 as the most pressing risk for CEOs in Europe and North America, including six of the ten largest economies in the world. These represent regions that are highly dependent on the use of technology to run their economies and businesses and have also been subject to multiple and notable cybersecurity incidents over the past year, including ransomware that was used to attack prominent industrial and manufacturing companies, as well as breaches of digitised public services. With growing digitisation, cyber attacks are becoming more lucrative for attackers who use an increasing array of sophisticated tools, and more dangerous for victims. The World Economic Forum cautions that detecting, defending against and deterring new cybercrimes is as important as managing known threats.

A matter for the board

Such are the magnitude of cyber risks that no business can afford to rest on its laurels. Every organisation faces risk, including financial, reputational, operational, environmental, regulatory and legal risks. Now more than ever, security risks need to be added to that list. It needs to be given the same weighting as all other risks and therefore the same level of operational oversight. Cybersecurity risk is not just an IT issue. It needs to be firmly on the agenda of board executives so that it is given the attention that it deserves, security programmes are adequately funded and a culture of security can be driven throughout the organisation. By adequately managing cybersecurity risks, the magnitude of damage can be reduced.

In order to do this, executives with cybersecurity management skills must be hired and given the prominence in the organisation that is needed. This is essential for guiding organisations in the switch in thinking that is required. Such executives will understand that security is more than a compliance tool. Cybersecurity tools can literally save a business – but only if they are operated and managed effectively. The landscape is shifting and savvy business leaders are needed who can help the organisation to move with the times and respond to threats in a quick and efficient manner. They must recognise the change from just investing in tools to procuring expert services that can keep their businesses safe.

The expanding attack surface and increasing complexity

As businesses are increasingly being driven by technology, control over that technology is being lost. As little as ten years ago, most technology was deployed within the walls – and control – of organisations. The walls of the organisation were once a hardened perimeter where access could be tightly controlled, but that is no longer the case. Organisational networks are increasingly hybrid in nature, bridging in-house technology with the use of public and private cloud services, mobile endpoints and increasingly interconnected tools, such as those that make up industrial networks. This greatly increases the available attack surface for adversaries.

The adoption of new technologies is essential to maintain competitiveness and for digital transformation initiatives that aim to take advantage of the power of digital technologies. But it is not just organisations that are looking to take advantage of the latest advanced technologies. Attackers are increasingly using artificial intelligence and machine learning algorithms to make their attacks more successful, along with increased use of bots to automate their tasks. Organisations need to make use of such technologies themselves and provide greater resilience.

> **“...cyber attacks are seen in 2019 as the most pressing risk for CEOs in Europe and North America, including six of the ten largest economies in the world.”**

The fear of being hit by a cyber attack or actually experiencing one can galvanise an organisation into action, providing the awareness that is needed for increasing investment in cybersecurity tools. But it also leads to a scramble to invest in point products to solve particular pain points. As many security practitioners will attest, this leaves them struggling to manage too many tools that are often not integrated, preventing them from having visibility over their security posture.

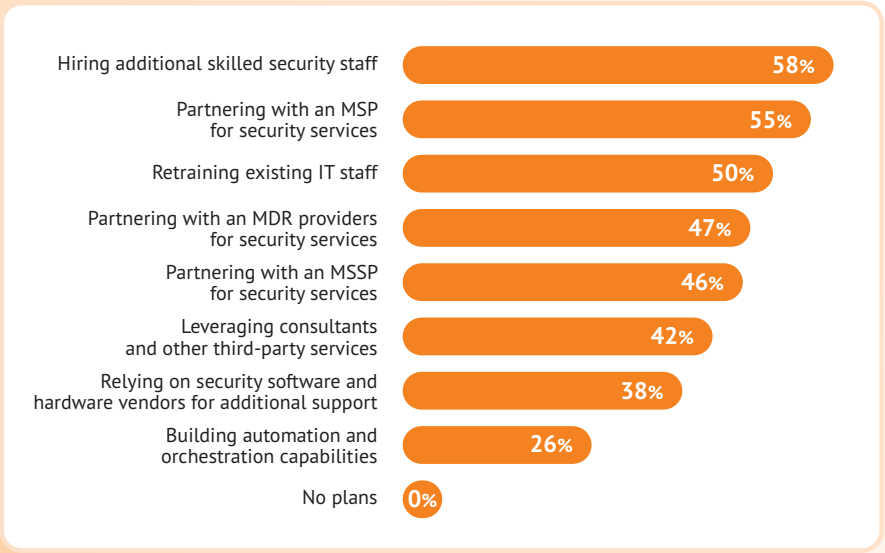

Figure 1: How are you bridging the skills gap? (Source: 451 Group)

Given the nature and volume of the threats that they face and the need to adopt new technologies to drive digital transformation, many of the tools that organisations must purchase to bolster security are extremely complex in nature, often needing more knowledge and expertise to handle than the standard tools that were traditionally available and that are no longer sufficient. According to Trend Micro, the security tools that are available today must be able to contextualise and analyse indicators of compromise to dig deeper into what really happened and how. Such technologies must be learnt, deployed, integrated and optimised to be effective, yet 47% of organisations surveyed by FireMon report that they are unable to learn or utilise complex new technologies to their full potential. Technology can only add real value if it can be used effectively.

Many such tools are also expensive to procure, draining already tight budgets. Fairly recently, endpoint detection and response (EDR) technologies have come onto the market to help organisations better detect and respond to threats impacting endpoints, which are a favourite target for attackers. Yet, research by Sophos has found that organisations have struggled to use such tools, with 54% saying that they are unable to get the full benefit from their investments, a figure that cuts across organisations of all sizes.

Skills shortages a drain on investments

Organisations report that they are finding it a challenge to hire and retain experienced security personnel who understand the new technologies that they wish to implement in order to elevate their cyber defences. Estimates of the global shortfall in skilled security personnel vary, but ISC2 has recently estimated that the number of unfilled security practitioner positions is as high as four million. According to research by the 451 Group, 78% of organisations are facing a skills and expertise gap in security. This is impacting organisations of all sizes, even among the largest enterprises. At the midmarket level, many firms have just a director of security and perhaps one or two security analysts, leaving them with no capacity to deal with alerts, even though this sector tends to see highly targeted attacks.

The ways that organisations are trying to resolve this situation are shown in *Figure 1*, which indicates that many are looking to outsource security functions. However, 58% are still relying on hiring new staff, which is unlikely to lead to a positive change in their circumstances.

Given this situation, is outsourcing security functions a good idea? Will the service provider not be facing the same staffing problems?

According to Trend Micro, skilled incident responders find it more exciting to work for a services firm such as an MDR provider that does hundreds of investigations per year. This is echoed by Cynet, which states that it has no difficulty recruiting staff, but that its customers – especially in financial services, manufacturing, energy and retail sectors – experience great difficulty doing so. F-Secure provides it staff with ample opportunities to spend time on research, leading to a better career path and skills development for them.

How and why MDR services have evolved

The ability to detect threats hidden deep in networks depends on detailed analysis of log and event data from a wide variety of sources—endpoint, network, cloud and systems attached to the network.

Many organisations have become dependent on security incident and event management (SIEM) systems, but found that they had many limitations in terms of data that it could ingest and therefore analyse, including insider threats and those using remote endpoints as an attack vector.

Advanced analytics and machine learning techniques enable a deeper level of insight to be gained from event data, greatly enhancing the capabilities of such tools. This has led to the development of complementary technologies, including endpoint detection and response (EDR), security orchestration, automation and response (SOAR), user and entity behavioural analytics (UEBA) and network flow analysis. But this also adds greatly to the complexity that organisations must manage.

This complexity, along with the demands placed on short-staffed security operations teams, has meant that not all organisations were able to realise the value of their investments in security tools.

MDR services not only relieve the burdens on organisations, but ensure that they are better able to face up to the threats that they face in an efficient and effective manner. They will help organisations to close security gaps and prevent them from becoming the next salacious headline.

> **“Organisations report that they are finding it a challenge to hire and retain experienced security personnel who understand the new technologies that they wish to implement in order to elevate their cyber defences.”**

Why not just go with an MSSP?

> **MDR services are designed to go above and beyond the services offered by traditional MSSPs.**

The use of managed service providers has been growing rapidly since they came to prominence in the 1990s and continues to grow. It is a form of outsourcing that enables organisations to improve their operations through access to external skills and resources in order to cut expenses. Among the key factors for considering the use of managed service provider are cost, quality of service and avoidance of risk.

Managed security service providers (MSSPs) are used by organisations of all sizes, providing a systematic approach to managing their security needs. They provide services such as round-the-clock monitoring and management in areas that include remote firewall configuration and administration, log management and analytics.

However, the use of MSSPs has its limitations as many of the services offered are generic in nature, being generally limited to the monitoring of security infrastructure. Although many offer a stable of technologies that they can manage on behalf of customers, they are rarely focused on the specific needs of the customer and its particular environment. As such, they are generally unable to offer services such as extensive, tailored forensics, threat research and analytics, being rather focused on detecting known threats such as vulnerability exploits and high volume attacks. They are able to alert customers to anomalies that are detected, but are not able to help customers with prioritising and investigating alerts for anomalies that are uncovered. According to MDR provider Expel, MSSPs offer just another alert feed for organisations that already receive more alerts than they know what to do with.

Enter MDR services

MDR services are designed to go above and beyond the services offered by traditional MSSPs. MSSPs are primarily focused on preventive controls; MDR services are designed to offer proactive detection to enable threats to be more quickly identified and remediation advice and recommendations, providing a much higher level of guidance for organisations for their security needs. Whilst they do provide the 24x7 continuous monitoring of IT assets that MSSPs have traditionally offered, they provide a more specialised level of service that includes alert prioritisation, incident investigation and offensive threat hunting across feeds from endpoint, network, server and cloud data, including the detection of lateral movement across the ecosystem that indicates that a threat has gained a foothold.

A key factor differentiating MDR providers from traditional MSSPs is in the use of the word *"services"*. MDR providers provide organisations with access to advanced technology, whether that be their own, that provided by a partner or controls that an organisation has already invested in, combined with access to a range of expert security professionals that can offer services tailored to an organisation's specific security needs in the areas of detection and response through direct interaction with the organisation. This is essential for organisations that face difficulties hiring and retaining experienced security practitioners. Through direct interaction with the organisation, an MDR provider's staff can provide services that are tailored directly to the organisation's needs, often with a dedicated person assigned to that particular organisation. With this, they provide a high touch, people first approach.

What constitutes MDR services?

MDR refers to a threat monitoring, detection, incident analysis and response service. It acts as an extension of an organisation's security operations team, whether as a virtual SOC or auxiliary expertise. MDR services can help an organisation to get the best out of existing technology investments, or help with the deployment and use of best of breed technologies.

MDR services collect telemetry from an organisation's environment, including its network, endpoints, cloud services and user activity, and correlates and analyses it in conjunction with threat intelligence services. Working not only in a reactive mode, threat hunting services can use offensive security techniques to proactively uncover hidden and unknown threats.

Experts from the service provider can then help the organisation to define and execute the best response to threats, events and incidents uncovered. Automation and orchestration capabilities are required for the most efficient and effective response. Other aspects that are routinely part of MDR services include machine learning, user behaviour and big data analytics.

> **"Through direct interaction with the organisation, an MDR provider's staff can provide services that are tailored directly to the organisation's needs, often with a dedicated person assigned to that particular organisation."**

Benefits of MDR services

Many of the technology tools that have been developed for dealing with complex, sophisticated security threats and incidents are expensive to purchase, implement and maintain, and require customisation to meet the specific requirements of an organisation. This requires advanced skills that most organisations do not have at their disposal.

MDR services provide access to a team of experts at a price that organisations can afford and enable them not only to better detect and analyse threats, but to stop them in their tracks before extensive damage can be done. They will provide much greater peace of mind for organisations that are struggling to keep their houses in order, offering a cost-effective adjunct to in-house capabilities to help improve the security posture of any organisation.

MDR services provide access to a team of experts at a price that organisations can afford and enable them not only to better detect and analyse threats, but to stop them in their tracks before extensive damage can be done.

Summary

Today's sophisticated and complex security threats require a swift, coordinated response by their victims. For many years, organisations have relied on an arsenal of technology in order to outgun their adversaries. As those tools multiply and deploy ever more advanced techniques in an effort to stay ahead, many organisations are finding themselves playing a game of catch up with the limited resources that they have at their disposal to handle them. MDR services provide an attractive alternative, giving access to expertise as and when needed to stack the odds in their favour in terms of detecting and responding to threats. Whatever the size or needs of an organisation are, MDR services could provide the lifeline that they need to stay afloat.

FURTHER INFORMATION
Further information about this subject is available from
https://www.bloorresearch.com/2020/03/what-is-mdr-and-why-is-it-needed/

Whatever the size or needs of an organisation are, MDR services could provide the lifeline that they need to stay afloat.

About the author

FRAN HOWARTH
Practice Leader, Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including ***Silicon***, ***Computer Weekly***, ***Computer Reseller News***, ***IT-Analysis*** and ***Computing Magazine***. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of ***InfoToday***.

Bloor overview

Technology is enabling rapid business evolution. The opportunities are immense but if you do not adapt then you will not survive. So in the age of ***Mutable*** business Evolution is Essential to your success.

We'll show you the future and help you deliver it.

Bloor brings fresh technological thinking to help you navigate complex business situations, converting challenges into new opportunities for real growth, profitability and impact.

We provide actionable strategic insight through our innovative independent technology research, advisory and consulting services. We assist companies throughout their transformation journeys to stay relevant, bringing fresh thinking to complex business situations and turning challenges into new opportunities for real growth and profitability.

For over 25 years, Bloor has assisted companies to intelligently evolve: by embracing technology to adjust their strategies and achieve the best possible outcomes. At Bloor, we will help you challenge assumptions to consistently improve and succeed.

Copyright and disclaimer

Bloor Research International Ltd
20–22 Wenlock Road
LONDON N1 7GU
United Kingdom

tel: **+44 (0)1494 291 992**
web: **www.Bloorresearch.com**
email: **info@Bloorresearch.com**