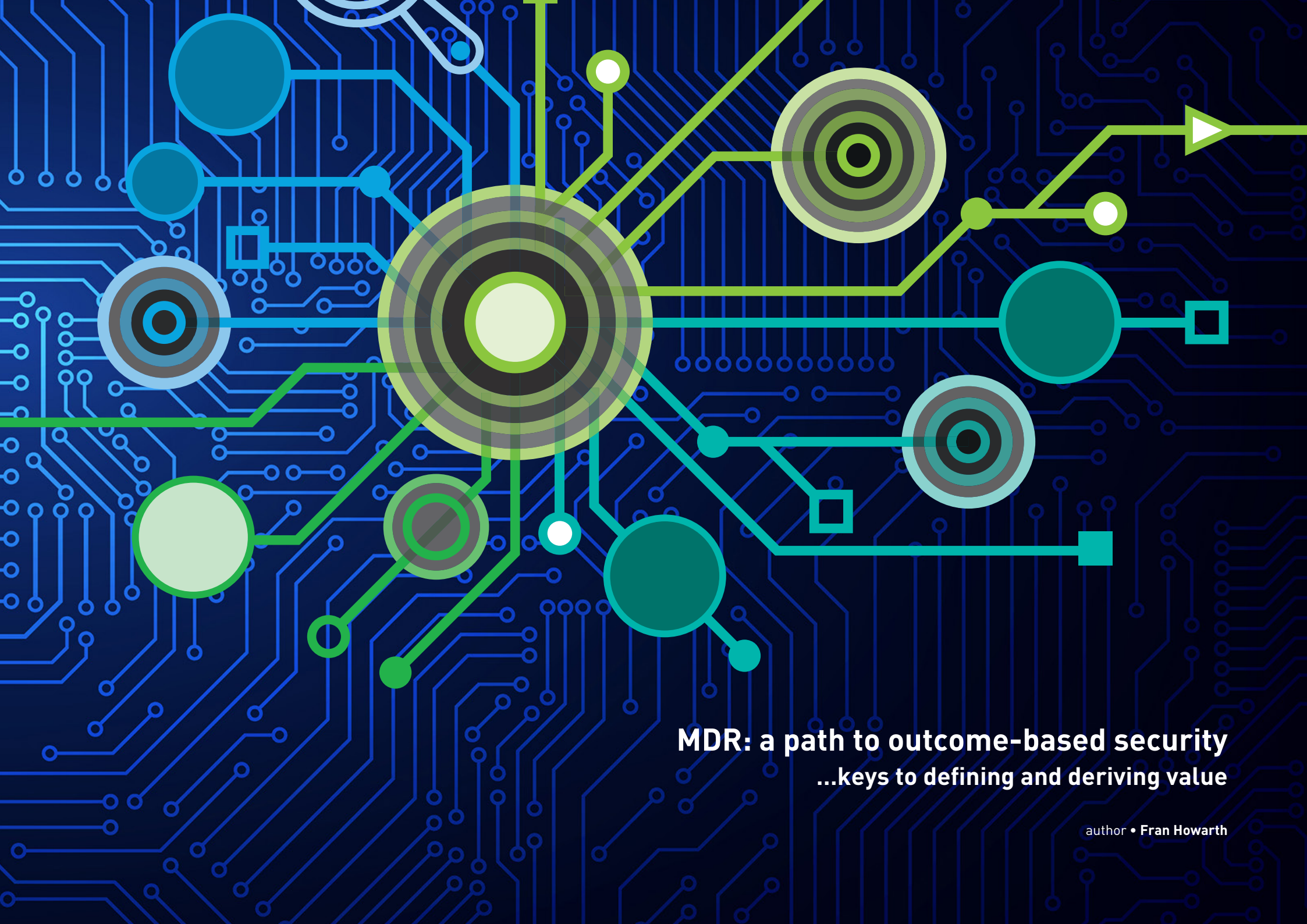


MDR: a path to outcome-based security

...keys to defining and deriving value

author • **Fran Howarth**

Executive summary

Multifaceted threats, complex technology solutions, difficulties in hiring and retaining qualified security staff, and the need to keep businesses running in the face of adversity are problems that the vast majority of organisations are grappling with on a day-to-day basis. Detecting and responding to threats before real damage can be done in such an environment is a challenge that many cannot meet. This gap cuts across organisations of all sizes in all industries.

Managed detection and response (MDR) service providers have stepped into this void. They help organisations cut through the complexity while acting as an extension of an organisation's security team, as and when they are needed. Whilst there are many vendors in an already-crowded market and there are also different flavours of services that they offer, there are non-negotiable capabilities that must form the basis of any viable MDR service.

According to Jack Danahy, Alert Logic chief evangelist, *"Security services, like MDR, will consume 75% of security spending within this decade."* To improve the effectiveness of that spending, this eBook aims to guide organisations in the practical issues that they should consider when evaluating and selecting a service provider to ensure that the security outcome lives up to their expectations.

The bottom line

For some, handing over responsibility for something as critical as security to a third party may seem like giving away the keys to the kingdom. But few organisations are in the position to go it alone given the multiple challenges that are involved. MDR services reduce the pain and cost of ensuring solid security and can help organisations to shore up their posture, not only in terms of current threats, but with a view to those we can expect in the future. By taking into account the practical considerations outlined in this eBook, organisations will be better informed as to what they should demand from an MDR service provider.

Fast facts

- MDR services must provide a proactive response to the threat landscape that organisations are grappling with, helping them to reduce the likelihood that an attack against them will be successful and ensuring that they are even shielded from previously unknown threats as they appear.
- MDR services must help organisations cut through the complexity of the technology that they have invested in, providing appropriate responses to threats detected. The ability to understand the impact of multifaceted threats on a particular organisation requires the intervention of humans and the intelligence that they can add to events seen. The ability to add human intelligence to automated actions is a key factor to consider.
- MDR services must be comprehensive enough to ingest telemetry from all the assets that make up dynamic environments that extend outside an organisation's perimeter to provide visibility over the entire estate. Without that visibility, organisations are left with blind spots, and are fighting a losing battle.
- MDR services must provide context regarding events so that responses are customised to meet to the needs of an organisation's specific environment, taking into account not only its technology infrastructure, but the business environment in which it operates and the concerns that it has.
- MDR services must provide reports that are useful and accessible to all in the customer organisation, from technical staff up to the board, to provide guidance to all and to provide ease of mind for executives that the best efforts are being made.

What is driving the need for MDR?

Achieving a measurable and desired security outcome may seem like a standard that cannot be reached. Among the most desired security outcomes are decreased detection and response times for security events, tailored protection against attacks, the ability to manage incidents that do occur, and threat reduction that leads to an overall improvement in the organisation's security posture. They all describe outcomes as measurable improvements in critical areas.

This desire for measurable improvement leaves many organisations grappling with a number of factors that make outcome-based security harder to achieve. These include a complex and sophisticated threat landscape that is increasingly hard to defend against. But it is not just the complexity of threats that organisations face. Rather, the current wave of technologies that are aimed at improving organisations' detection and response capabilities are hard to implement, manage and receive the desired results from. As many organisations are struggling to attract and retain skilled security practitioners, this can seriously dampen their efforts to achieve the outcomes that they desire.

Factors such as these have led to the emergence of MDR services, as shown in **Fig 01**. MDR service providers help organisations to cut through the complexity and provide access to expert resources who act as an extension to organisations' security teams, shoring up their threat detection and response capabilities. Further discussion of the need for MDR services and what they constitute can be found in a recently published Spotlight.

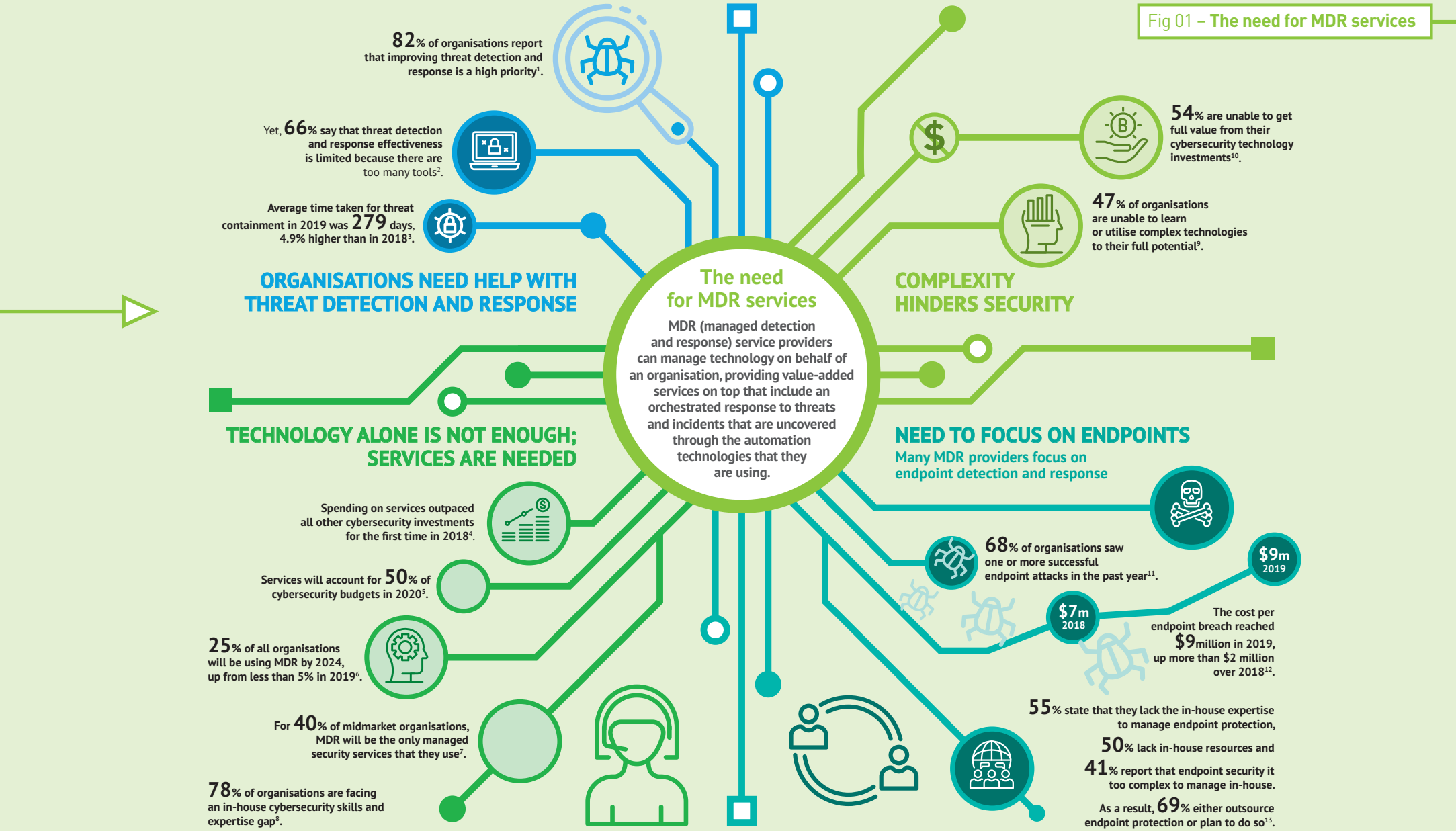
"Just like how cement binds together different materials in construction, we need similar 'binders' to bring together technology and skilled security officers to create an integrated security solution."

Sun Xueling,
Senior Parliamentary Secretary for Home Affairs and National Development, Singapore

MDR services help organisations to solve a defined set of issues to address their biggest pain points. MDR service providers work alongside security resources from the customer, providing access to a custom-built, integrated platform that can help customers to cut through complexity to achieve the desired security outcome. Building a security operations centre (SOC), including the cost of hiring and the cost of the equipment needed is daunting for any organisation and does not always achieve the desired results. MDR services are designed to help with these problems.

The use of MDR services brings benefits to a wide range of organisations, ranging from smaller firms that lack an in-house SOC to large multinationals that are looking for a better, more effective way to detect, analyse and mitigate threats and improve their security postures over time.

Fig 01 – **The need for MDR services**



Source:
1, 2 ESG, 3 Ponemon Institute, 4 Forrester Research, 5, 6, 7 Gartner, 8 451 Research, 9 FireMon, 10 Sophos, 11, 12, 13 Ponemon Institute

Practical guidance for what MDR services should offer

Not all MDR services are the same. Some are offered by technology vendors that have developed their own technology, of which endpoint detection and response (EDR) is the most common, and offer services to help customers get the most from those investments; others are considered to be technology-agnostic. In this latter case, vendors also often include EDR capabilities, generally from one or more third-party vendors, and have built telemetry platforms that ingest feeds from a wide range of technologies and devices that constitute an organisation's extended network.

However, there are common capabilities that all MDR services should offer in order to provide real value to customers in terms of being able to dramatically improve their threat detection and response. Alert Logic recently released its MDR Manifesto **[see here]**, which identifies seven tenets that all MDR services should adhere to, as shown in **Fig 02**.

The remainder of this eBook looks into the tenets or principles of MDR in greater detail, examining what they mean in practice in terms of MDR services delivery.

Response to the threat landscape

Faced with a complex and constantly evolving threat landscape, MDR services must help organisations to both reduce the likelihood or impact of successful attacks, as well as ensuring that they are staying abreast of new threats and vulnerabilities as they are uncovered through research – as described in tenets **1** and **3**.

Staying ahead of current threats is a daunting task for any organisation. Many adversaries continue to exploit publicly known software vulnerabilities for which remediation is available. Using old vulnerabilities requires fewer resources and is lower cost than developing zero-day exploits. These attacks continue to succeed because, while most security practitioners understand that managing patches and updates are key security tasks, it is time-consuming and problematic to know where to prioritise action. This is exacerbated by a lack of visibility into all assets that make up extended networks and their level of security readiness, leaving blind spots about what versions of software are deployed in what location and on which devices.

When an attack does occur, organisations are finding that they are getting more complex and harder to defend against. Attack vectors were historically divided into internal and external sources, but those lines have become increasingly blurred. Phishing employees is a preferred method of attack for external adversaries, who look to use an initial success

Fig 02 – **The seven tenets of MDR**

Source: **Alert Logic**

in gaining a foothold on the network to burrow deeply within it, moving laterally in search of greater gains. Keeping a vigilant eye on all stages of the attack lifecycle requires a level of visibility that many organisations cannot achieve by themselves.

Yet, it is not only existing vulnerabilities that are being exploited or traditional methods of gaining entry that organisations need to defend against. The threat environment is never static and some adversaries are looking to stay ahead of the game by using tactics, techniques and procedures that evade defences and leave few forensic artefacts. A high level of expertise is required to detect and recover from such attacks—and this is something that many organisations lack.

Already under-resourced and playing a game of catch up with adversaries, security teams these days are finding that they have even more on their plates. A recent survey of IT and security professionals worldwide by Check Point Software found that 95% of respondents stated that the Covid-19 pandemic has created additional security challenges that they must deal with, including secure remote access and increased use of shadow IT, whilst 71% reported that they have seen an increase in security threats and attacks since the outbreak. This is backed up by data from Google that shows that 18 million Covid-19-related malware and phishing emails are being seen every day, which can expose internal user mistakes, configuration errors and other problems that can be exploited.

As shown in **Fig 03**, the consequences of failing to prevent and respond to security attacks can be far reaching. As a consequence, cybersecurity issues are getting more attention among senior executives who see that it is becoming a business imperative. Yes, even while it is becoming a top priority, improving security is expected to happen alongside transformational initiatives, and thus remains under-resourced.

Fig 03 – **Consequences of a successful attack**

Tom Adams, Aptum:
The consequences of a successful attack can be summarised in four broad categories:

FINANCIAL – including the direct costs of a breach, the impact of trading systems being taken offline so that it is unable to generate revenue, or the need to pay compensation to those impacted.

COMPLIANCE – a security incident that leads to an organisation being non-compliant with regulatory mandates could have a very serious business impact. Being able to demonstrate that they have the best possible security controls in place is a key aspect of achieving and maintaining compliance, and MDR services can help with that.

TRUST AND REPUTATION – although it is not easy to quantify, breaches can have long lasting reputational impacts and can destroy trust in brands. This is a significant risk that sits in the background of most business leaders' minds.

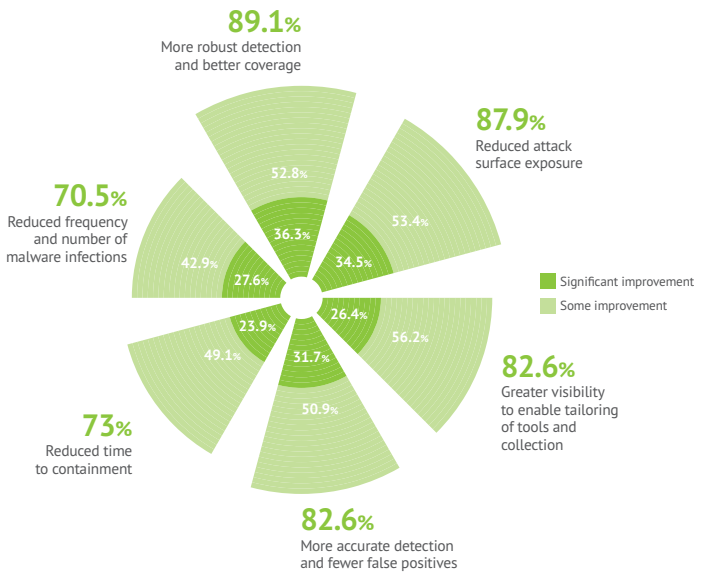
BUSINESS CONTINUITY – some types of attack have the potential to cause entire systems to be shut down, to be taken offline, or to destroy data. Can an organisation survive a serious incident and remain viable if it loses access to data and critical applications? We see MDR as being almost a pillar of IT and business resiliency alongside things like disaster recovery.

Source: **Tom Adams, marketing director Aptum**

How MDR services can help address the threat landscape

One of the services provided by MDR providers is continuous scanning of the network and endpoints, looking for known vulnerabilities and potential exposures. This will enable old, unpatched vulnerabilities, unauthorised applications, risky configurations and out-of-compliance devices to be uncovered. The aim is to detect threats before they can become an incident. But that is not always possible. Acting as an extra set of eyes, when threats are uncovered, the service provider will offer expertise regarding the impact and severity of threats seen and will offer tailored remediation guidance.

Fig 04 – **Improvements seen from threat hunting**



Source: **SANS Institute 2019 threat hunting survey**

However, MDR services can go much further than just identifying and helping to remediate threats and vulnerabilities that are already known about. Continuous research is necessary for uncovering and understanding unknown and evolving threats. This has led to the development of threat hunting services by MDR providers, with the aim being to get a complete picture of all threats impacting an environment.

Threat hunting combines the use of machine learning and behavioural analysis techniques that delve into information to find indicators of compromise and suspicious activity such as lateral movement across a network combined with the use of threat intelligence to understand the tactics, techniques and procedures used by attackers. Using a mixture of human expertise and automation, the role of humans is to generate alerts regarding attacks that go undetected by automated tools. Threat hunting provides organisations with a better chance of catching an attack early in order to limit the resulting damage.

Threat hunting goes hand in hand with threat intelligence, which gathers information on the latest threats from internal and external sources. It helps organisations with information pertaining to the current threat landscape, which they can analyse to look for the most appropriate actions to take. However, many organisations struggle to get actionable intelligence from raw data feeds as they lack the ability to integrate threat intelligence into their technology environment, and do not have sufficient experienced staff and robust enough processes to be able to use the information to make informed decisions.

MDR services help to bridge those gaps by providing the ability to ingest feeds from multiple technologies and systems and the expertise to make sense of them. This is invaluable to organisations looking to reduce the likelihood of successful attacks and ensures that the latest threats are taken into account, with pointers as to how their specific environment is impacted.

"We are constantly monitoring things like configuration of their environment. Are they drifting away from security best practices? Did somebody push a change that is causing a new vulnerability?

Instead of asking the customer or business "Are you 100% secure?", the question should be "Are you confident that, in the inevitable circumstance that there is some sort of threat detected, you have the right people, processes and tools and the approach to be able to rapidly identify the issue, immediately mitigate it and move forward with confidence?"

So, reduce uncertainty, increase confidence and have an operationalised view of security. That's the success of MDR for me."

Jonathan LaCour, CTO, Mission

Augmenting technology with human intelligence

As has been noted, gaining actionable intelligence from raw data feeds is an arduous task. Tenet 4 of the MDR manifesto argues that it is imperative that technology be augmented with human intelligence to ensure accuracy and value. Technology tools can help considerably, but most organisations do not have the level of expertise that is needed in-house to make the best use of them, limiting their capabilities in threat detection and response.

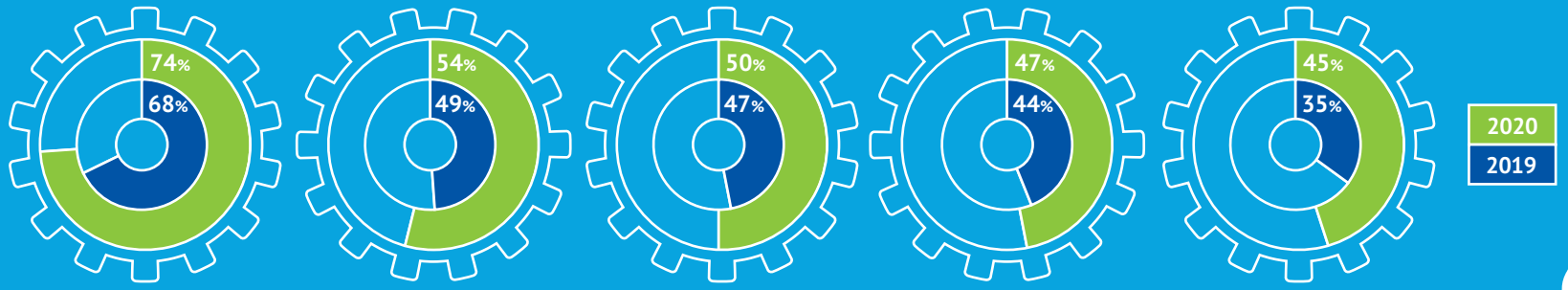
"Only a human can understand how an organisation is really set up, what its goals are, and how those goals can be achieved from aligning with security best practices."

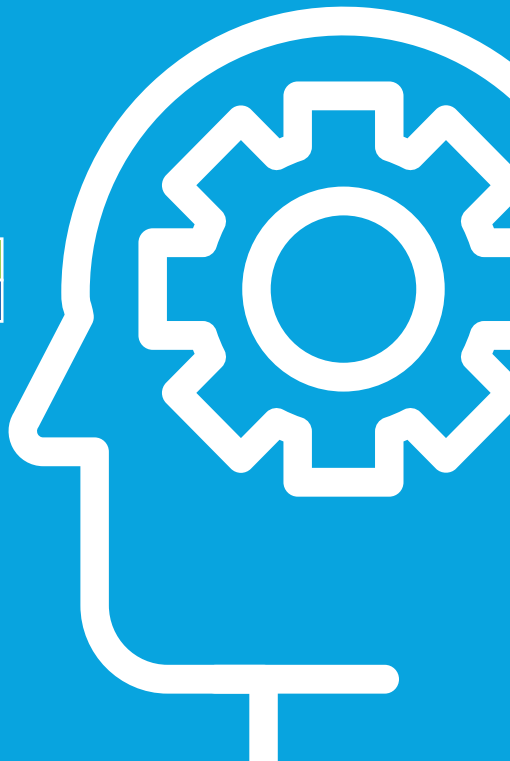
Ron Hayman, chief cloud officer, AVANT

Although many detection and response technologies incorporate machine learning or even robotic process automation, they do not always enable organisations to get to a position of comfort in terms of enabling a machine to take a disruptive action, such as disabling an account or disconnecting a system, which could impact business operations. For most organisations, threat detection and response is not a core competence and they face large gaps in dealing with something that they are absolutely not experts at. They would rather focus on moving the business forward.

As **Fig 05** shows, there are many areas in which automation alone falls short. Humans are required to improve outcomes.

Fig 05 – **What automation will NOT improve for security staff**





Source: **Ponemon Institute** ***The 2020 Study on Staffing the IT Security Function***

How MDR services can help augment technology with human intelligence

The human element is important for adding information and context to existing controls that an organisation has in place or the MDR services provide. This helps to prioritise where action should be taken first to drive faster incident investigation and response, taking into account the needs of a particular organisation.

MDR services can help with the aspects of technology that few organisations can manage on their own. They can help to bridge gaps by having their experts work as an extension of the security team for their customers, providing the expertise needed to make sense of data feeds. According to Drew Lydecker, president and co-founder of AVANT Communications, MDR providers are in the position to guide their customers because they understand and assist a variety of customers day in day out, and benefit from that diversity of challenges.

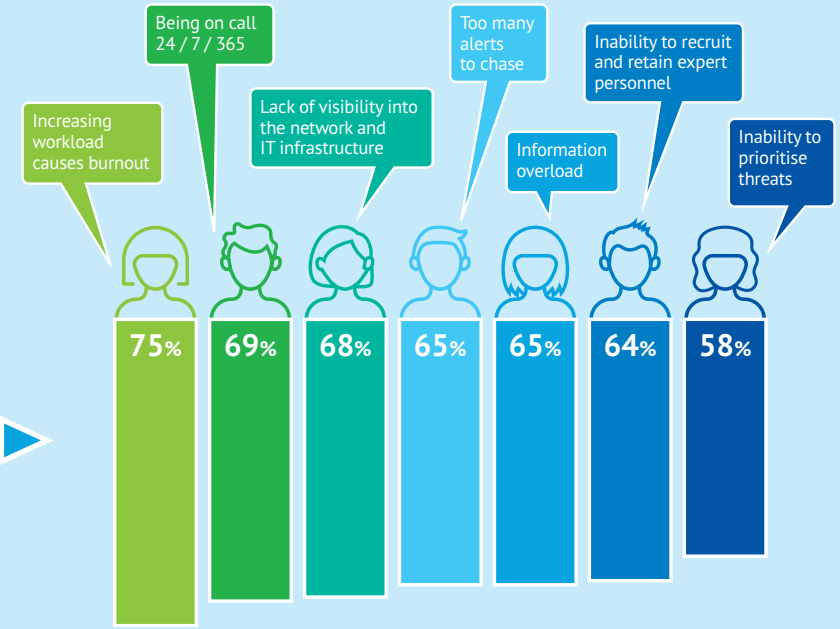
These human resources are attracted to this kind of work, and few, if any, MDR providers report that they have problems recruiting and retaining experienced and qualified staff. The varied and interesting work that they offer and the ability for personnel to advance their skills are real draws for practitioners who are looking to work in such environments and is key to why such providers are able to attract and retain talent. This makes an MDR provider an ideal place to work compared to security teams within end user organisations, offering clear career prospects and the opportunity to see that they are making a real difference.

As part of this, many MDR providers employ a vast army of security researchers and analysts who are encouraged to spend some 50% of their time researching the latest threats in addition to gaining greater practical experience from providing services to customers. This greatly helps them to keep abreast of the fast-moving security landscape and to ensure that the advice that they give is as accurate and valuable as possible. The insights that they gain through performing advanced research can then be integrated into the services that they offer, enabling their services and coverage to be improved with the benefit of insights gained from human intelligence.

Cover all assets and scale across dynamic environments

The importance of ensuring that all assets in the organisation are actively being monitored at all times cannot be understated. Tenet 2 states that MDR services must provide 24/7 visibility and cover all assets in an organisation. This can be taken together with Tenet 6, which states that such as service must scale to deliver technical analysis and human insights across dynamic environments.

Fig 06 – **What makes working in a SOC so painful?**



Source: **Ponemon Institute,** ***The economics of SOCs 2020***

The two can be taken together since no organisation is an island and must extend its network to incorporate all manner of stakeholders, from employees to supply chain services, and this extended network can end up being very widespread. In the majority of organisations it encompasses the use of cloud services, often multiple variations thereof, and any number of remote devices.

As **Fig 06** shows, lack of visibility is cited as a key factor in making the work of security practitioners in a SOC more difficult, since it impedes their ability to detect and respond to all the threats that the organisation faces.

No organisation can confidently assert that they have achieved 100% security. Even with the right tools and processes in place, organisations are still vulnerable if comprehensive visibility across all assets is not available at all times. Performing vulnerability scans, patching systems in a timely manner and repairing misconfigurations are all considered to be best practices, but are extremely time-consuming and seldom performed universally. Further, if an organisation is hampered by an inability to look across the entire estate at feeds from all systems to provide a holistic view of the environment, it is likely that there will be problems that could become an Achilles' heel—devices with open ports, configuration errors, new vulnerabilities in newly deployed software or critical vulnerabilities that are missed that could be exploited by hackers.

"Perimeter is the wrong parameter."

Tim Femister, VP digital infrastructure, ConvergeOne

Visibility can be hindered by many things. The fear of being hit by a cyber attack or the scramble to respond to an incident have led many organisations to invest in point products to fill particular gaps, leaving them to struggle with the management of too many tools that are generally not integrated, hindering visibility and creating blind spots. In some cases, systems that have been implemented, such as security incident and event management (SIEM) systems, have not always lived up to their promise owing to limitations in what data they can ingest and analyse, with particular problem areas being the ability to identify insider threats or threats using remote endpoints as an attack vector. Newer technologies that include EDR, security orchestration, automation and response (SOAR) and user and entity behavioural analytics (UEBA) add to the complexity that organisations must manage, hindering visibility.

The widespread use of hybrid environments adds to the challenges that they face, both in terms of extending the network beyond an organisation's control and the fact that many services in such environments are provided by external service providers such as SaaS services. Many security executives are keenly aware of security problems that can be caused by external services, such as insufficient oversight of who is accessing what. These hybrid environments remove the convenient logical security demarcation point at the boundary of a network.

How MDR services can help with visibility and scale

The continuous monitoring that MDR service providers offer is a key part of achieving visibility across all assets in an organisation. Some have built platforms that scale to ingest telemetry feeds from multiple sources. These should include event data from endpoints, netflow, packet data and metadata from network systems, access and authentication events, data feeds from cloud services, and data regarding any vulnerabilities found.

Scale also refers to the ability to add new feeds from new technologies that are implemented and to incorporate data pertaining to vulnerabilities and threats that are uncovered, including information on tools, techniques and procedures being used by adversaries. But scale can further refer to the number of humans needed to run the service effectively, which must be sufficient to analyse and make sense of massive volumes of data and to ensure that timely and comprehensive reports are made to customers. This is where MDR services can really help as they have the human resources and intelligence available to ensure continuous development of the service and to provide the expertise as and when it is needed.

"Organisations are struggling with just getting the right people to help them and also the scale and speed. The cloud allows you to move fast and people are adding so much to their managed infrastructure in AWS. We are finding that customers are not able to keep up with the growth that they are seeing of their own business."

Rohit Gupta, global segment leader for security, AWS

Fig 07 – **The importance of telemetry**

The word telemetry comes from the Greek for remote and measure. In IT terms, it refers to data that is collected from multiple points to give a complete view of network activity. By gaining a complete view, organisations will be better able to effectively manage threats and make more informed decisions regarding what actions to take.

However, the sheer volume of data that must be collected from multiple sources makes it a challenge to make sense of the data. This is compounded by an ever growing array of data sources as data must be collected from endpoints, networks, security controls and cloud services. The data that must be collected includes NetFlow, packet capture, endpoint forensics, and log and event data to provide information about where data is flowing, from what devices and to what IP addresses. A key challenge is to narrow all that data into a tractable stream in order to find signals through the noise that can be used for targeted analytics.

It is beyond the means of most organisations to collect, normalise and analyse such huge data sources, which is where it makes sense to outsource to MDR providers, some of which are handling hundreds of terabytes of telemetry information per month. They will provide the eyes and ears that organisations need in order to understand how threats and vulnerabilities uncovered through analysis of such information impacts them, and what is the best response to take.

Contextual information is key

Tenet 5 states that MDR services must provide custom responses that reflect business and attack context and cause.

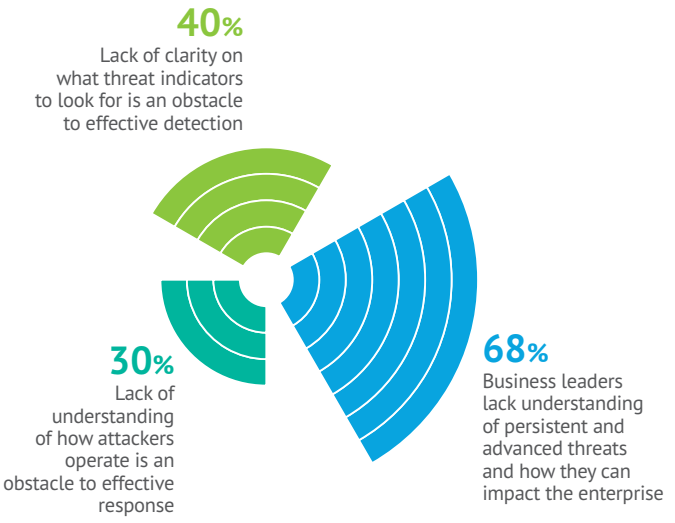
To gain context, supplemental information regarding an event is essential for improving security decisions both now and in the future and helps to ensure that better, more accurate and actionable security decisions that take circumstances into account are made that not only improve the overall security posture, but that support an organisation's operating requirements. Contextual information can include such things as location of user, the time an event occurred, IP address, type of device, URL and application reputation, business value information and the threat context in which any decision is made.

In preparing an attack, adversaries will often perform a great deal of research about their intended target and its infrastructure, such as physical and virtual systems, operating systems, applications, services, protocols, users, content and network behaviour. By gathering as much information as they can, they hope to gain an edge on those looking to defend their network and assets.

To counter this, an organisation needs to understand all the risks that they could face, taking into account the value of assets they are trying to protect, and the likelihood and potential severity of an attack. They must take into account all potential attack vectors, including endpoints, email and web gateways, virtual environments, cloud services and assets in on-premise data centres. All of these points generate alerts when incidents or unusual events are seen. As a result, many security teams are finding themselves overwhelmed by the volume of alerts that they receive, a large proportion of which are false positives. Organisations need a way to sift through all of those alerts to gain accurate and timely insights that are relevant to their organisational set up and the industry in which they operate.

As **Fig 08** shows, the greatest inhibitor into effective response is a lack of understanding of the context of attacks.

Fig 08 – **Threat understanding impedes multiple functions**



Source: **Ponemon Institute,** ***Managing risk of post-breach or resident attacks***

How MDR services can help with customising responses

The MDR service provider must work to gain an understanding of a particular organisation's environment and its business objectives so that they can recognise the scope and context of an incident in terms of how that organisation will likely be impacted. According to Tim Femister, VP digital infrastructure, ConvergeOne, the pace of change that organisations are seeing is staggering and is a major challenge for their customers. Security practitioners must have a human at the end of a phone line who they can actually talk to when needed and can scale up the response needed. This is a bonus for all organisations that are struggling to identify actionable information from alerts that they see and will help to provide a response that is customised to their needs.

Many technologies used today incorporate a great deal of context about what they uncover in an environment, along with machine learning to guide future actions based on patterns seen. The information that they provide gives context that can be applied to asset criticality and allows actions to be coordinated to manage business concerns that a particular organisation faces related to an incident such as legal and regulatory requirements, maintenance of customer communication, and avoidance of business outage and downtime.

Telemetry gathered from the extended environment does not only show an attack at a single point in time, but can also be correlated with historical data and threat intelligence to add context to events and to identify the particular type of attack that is occurring, such as whether or not data is in danger of being stolen, and the likelihood of considerable damage being caused. MDR providers will provide guidance based on what is being seen and its likely impact on a particular organisation so that the most appropriate response can be taken. In many cases, they will guide customers through the use of playbooks designed for responding to particular scenarios, helping an organisation to tailor the response to its particular needs.

Results and reporting must be credible

The seventh tenet from the MDR Manifesto states that MDR services must deliver results and reporting that are credible, accessible and useful.

Until fairly recently, the board of an organisation was rarely interested in cyber security reports. Security executives commonly reported that they were barely given more than one item or paragraph in terms of quarterly reports and even then scant regard was paid to what they had to say.

Times have changed. The board and other senior executives have come to realise that cyber security is as important as all of the other risks that organisations face, alongside operational, financial, reputation and legal risk. In fact, cyber security risk plays into all of these. A serious security incident can derail operations, have grave financial consequences, can seriously damage reputations and can put an organisation at risk of sanctions for non-compliance with the regulations that it faces. It is vital for the overall success of an organisation that it is able to provide reports on security that are credible and useful.

"The job for my MDR for me is to take raw data, consume it and come back with something that's much more succinct. Today, MDR is finally becoming a mature platform where I get a single pane or close to it and then I get very detailed and specific information back on where my threats are. That's really the goal at the end of the day: less people on my end. I rely on the MDR to hone that down and provide me with meaningful information. At the end of the day, that's the goal."

Peter Hoff,
CISO, large retailer

Left to their own devices – without complete visibility over their environment, knowledge of the latest threats and their likelihood of impacting their particular organisation, lack of staff to prepare credible reports and point-in-time snapshots – organisations struggle to articulate the exact state of affairs. This means that it is difficult to understand the true impact of cyber security on operations and to make effective decisions to guarantee the security of their overall operations.

How MDR services can provide a more credible picture

MDR service providers work to gain a deep and detailed knowledge of the security posture of their customers and the impact of security on their environment. They are constantly monitoring that environment, scanning across all of the assets that make up a network. They respond to, at a minimum, hundreds of events per year on behalf of customers. An effective response is based on well thought out, repeatable processes that are constantly being developed and refined according to type of incident.

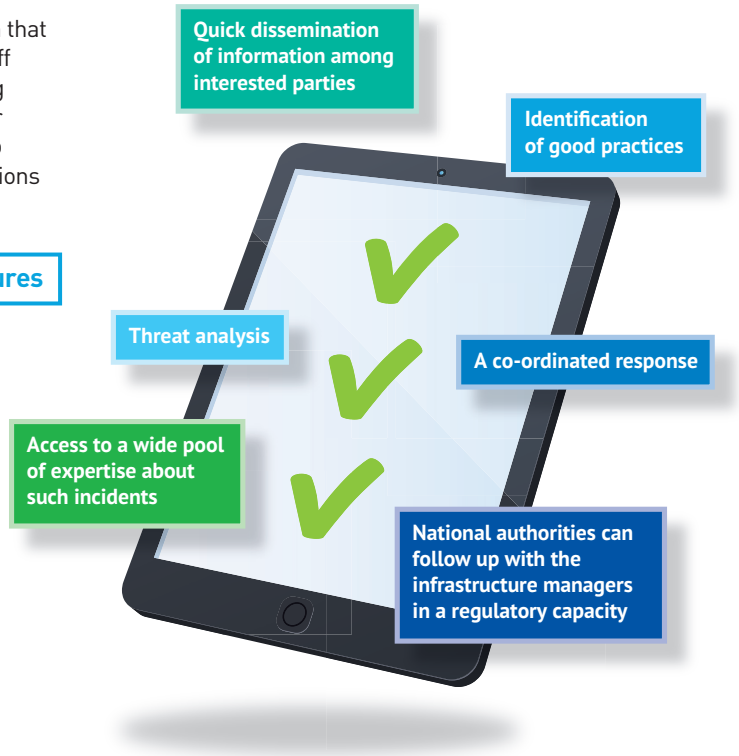
> ***"You need to have confidence in the reports that you're getting and that the information that you're getting is actionable and relevant to your business. That's a real challenge and where good reporting and good data make the difference as something that you can apply to your business. Every business is different and you can't have a one-size-fits-all solution."***
>
> *Curt Vurpillat, senior security consultant, Ingram Micro*

Because they build up relationships with customers and gain extensive knowledge of their environment and operational needs, they are able to ensure that the results seen from investigations provide the customer with needed support to help justify the investments that they make. But reports on the results seen can neither be provided at just one point in time, nor be on demand only. For best results, reports should be generated on a regular schedule where they can be discussed by all parties to learn from what has happened so that they can incorporate what has been learnt into processes designed to create greater resilience over time.

According to Peter Hoff, CISO of a large retailer, there has been a shift in recent years, as discussed above, regarding the information that an organisation's board is interested in. Hoff has seen a shift from information regarding how many viruses were seen in a particular period and what patching has been done, to broader discussions regarding the implications of security incidents, such as phishing. The data that is required for new reporting requirements should be provided by the MDR solution—something that he notes has been improving. But the information provided in reports should not only be useful for reporting to the board. Rather, it should be usable for lower end analysts, engineers and those in charge of keeping the network secure. The information has to be usable for those people, giving them the capacity to respond quickly without creating a bottleneck.

Fig 09 – **What effective incident reporting ensures**

According to ENISA, effective incident reporting contributes to the collection of reliable and up-to-date data on information security incidents. It ensures:

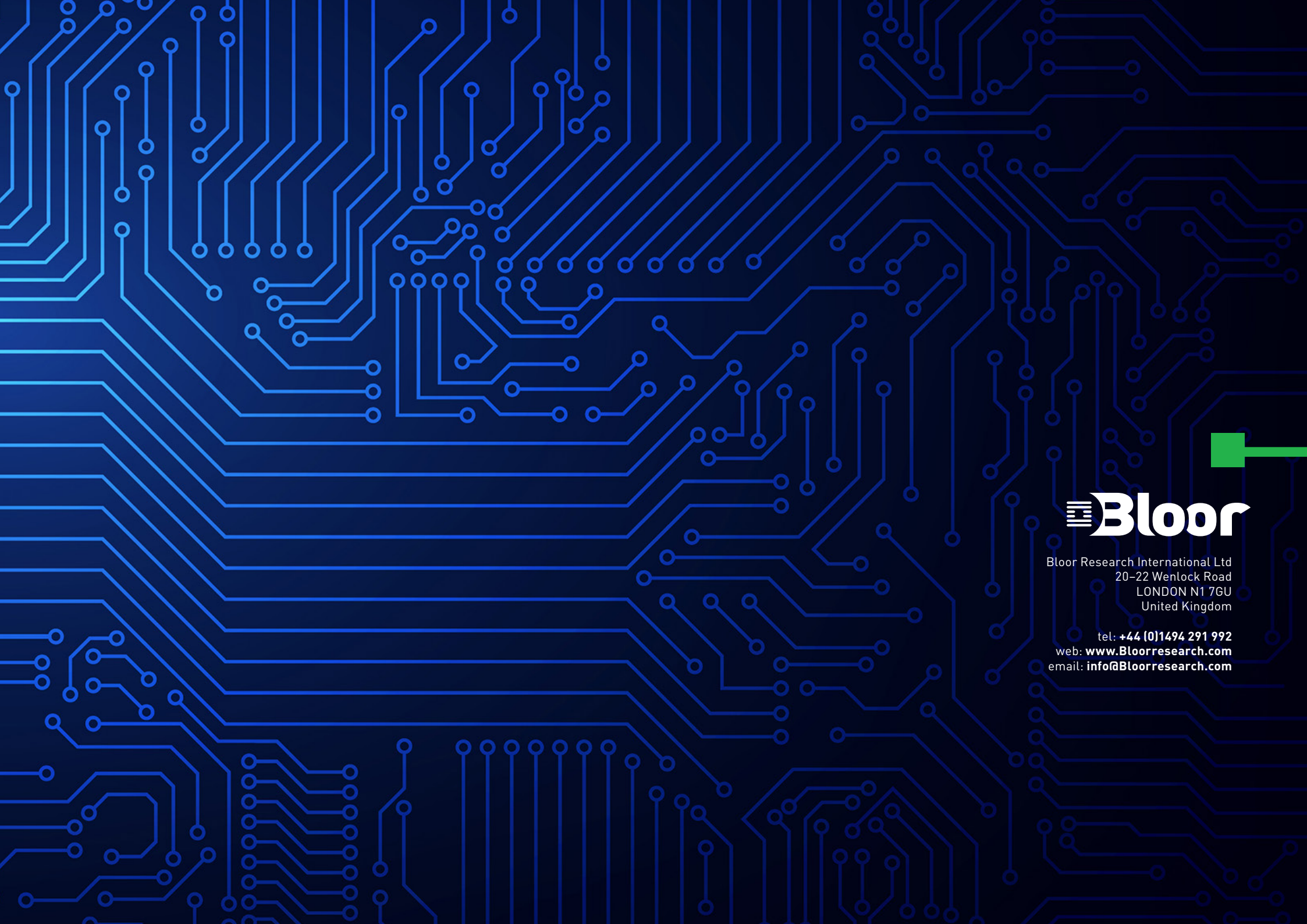


Closing summary

The use of technology has becoming a driving force in business, helping drive innovation and supporting the need for efficiency and profitability.

But investing in technology is not always a panacea. In the area of cyber security threat detection and response, the situation is complicated—and so is the technology that has been developed to help organisations to defend themselves. Investing in technology alone is no longer sufficient if an organisation is measuring those investments in terms of a more secure environment. Security services, informed on the best way to protect organisations and their technologies are essential.

MDR services answer these needs and are proving to be a boon for organisations in their efforts to achieve their goals in defeating adversaries and shielding themselves from harm. Looking under the covers, there are a number of key capabilities that all MDR services must offer if their promise is to be fulfilled.



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**