Phil Muncaster

November 2022

A BUYER'S GUIDE TO MANAGED DETECTION AND RESPONSE

What is it and why do you need it?

eset® Digital Security
Progress. Protected.

TABLE OF CONTENTS

SUMMARY

The corporate cyber risk landscape is rapidly evolving. Digital attack surfaces have significantly expanded thanks to pandemic-era investments. Cloud systems, distracted home workers, remote access infrastructure, distributed endpoints, and complex supply chains present large and attractive targets for threat actors. At the same time, the cybercrime underground is professionalizing with its own complex supply chains, malware-as-a-service offerings, and innovations in tactics, techniques, and procedures (TTPs).

Against this backdrop, threat prevention, while desirable, is not always possible. That's why organizations should consider evolving their approach to a more holistic one, based around prevention, detection, and response. This gives teams the capability to block malicious actors from entering and damaging their systems. And if prevention fails, they still have detection and response capabilities to spot suspicious events and resolve any threats before they can penetrate too far.

But which detection and response tool should organizations choose? Extended detection and response (XDR) can be useful, but this adds further challenges such as how to find and fund the security operations staff needed to operate it, without being overloaded with alerts.

Enter managed detection and response (MDR), a type of managed security service that combines tools, technologies, and cybersecurity experts to provide organizations with powerful detection and response capabilities. When done right, MDR offers a more effective way to manage cyber risk. But the critical factor is which vendor to partner with.

Organizations should consider providers with a proven track record of delivering high quality threat intelligence and technology with a high detection rate, a low false positive rate, and a light footprint. They should also consider customer service and the degree to which MDR can be optimized for specific needs of their organization.

XDR: HOW DOES IT WORK?

XDR is an evolution of EDR, which optimizes threat detection, investigation, response, and hunting in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management, cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation.

Source: Forrester, 2021

CURRENT CHALLENGES

In the ongoing arms race that is cybersecurity, it often seems as if our adversaries hold all the cards. They're supported by a cybercrime underground worth trillions of dollars annually, which provides all the tools, knowledge, and data needed to launch attacks with ease. Threat actors are often sheltered by hostile states, ensuring attacks can be launched without fear of reprisal from law enforcement. Furthermore, malicious software-as-a-service (SaaS) offerings have democratized the ability to coordinate audacious campaigns, even for groups with less technical acumen.

On the other side, chief information security officers (CISOs) and their teams are increasingly being pulled in several directions at once. Investments in digital transformation during the pandemic have significantly expanded the corporate cyberattack surface. **Remote working environments** represent a particularly dangerous visibility and control gap—encompassing everything from unpatched endpoints to distracted or negligent users. Yet many security teams are understaffed and overwhelmed by too many ineffective point solutions, which add complexity and reduce productivity.

The potential financial and reputational damage caused by a serious security breach has never been more acute. Yet the ability of organizations to effectively mitigate the risks associated with such incidents is, if anything, diminishing. Data breach costs globally stood at an all-time high average of over US$4.2 million in 2021. And according to one global insurer, a fifth of US and European businesses that suffered a cyberattack that year nearly became insolvent.

Against this backdrop, **100% prevention is simply not realistic**. A determined attacker will always find a way to compromise vulnerable targets. The focus must therefore be on complementing this approach with detection and response. Yet here too, organizations are falling behind. The average time it took globally to identify and contain a breach in 2021 was 287 days.

XDR uses behavioural analytics across endpoint, network, cloud, email, and other layers to spot suspicious activity and stop attackers before they can make an impact.

MDR is effectively an outsourced version of extended detection and response (XDR), sometimes combined with other tools.

Therefore, many organizations are turning to MDR—a type of managed security service combining tools, technologies, and cybersecurity experts. Half of organizations globally will be using MDR to contain threats by 2025, according to Gartner. However, while XDR requires the customer to do the monitoring, detection, and response, with MDR, a trusted cybersecurity provider takes care of the heavy lifting—freeing in-house staff to focus on high-value tasks elsewhere.

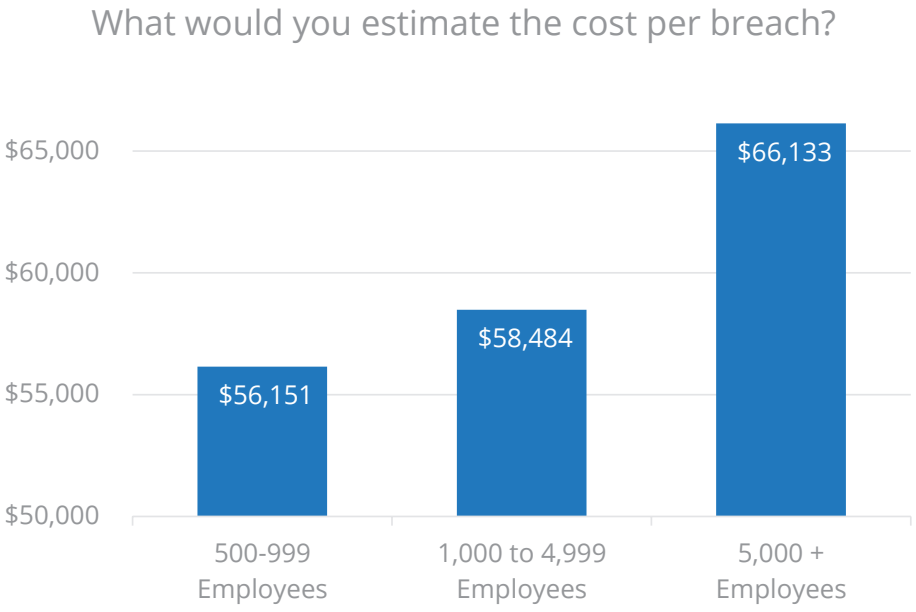
91%

of enterprises globally are using or plan to use deployment services, technical support, cybersecurity support, and cybersecurity threat hunting/monitoring as a service.

Source: Internal ESET Research Survey among 404 Enterprise-grade respondents.

BREACHES ARE A REALITY

IDC



Source: IDC, Security Services Market Update, 1Q22, Doc # US48907622, March 2022.

WHY DO YOU NEED MDR?

Although the average spending on cybersecurity doubled in 2021 for firms with 250-999 users, and surged 65% for enterprises with 1,000+ employees, breaches are happening today on a monumental scale.

In the US, 2021 saw a record volume of publicly recorded data breaches, 23% higher than the previous all-time high of 1,506. In the UK, 59% of mid-sized[1] and 72% of large businesses[2] said they detected breaches or cyberattacks in 2021. The ransomware threat is particularly acute: one report reveals over 623 million attacks were detected in 2021, a 105% increase on the previous year.

The corporate attack surface expands

Why are organizations struggling to repel adversaries? Partly because they're more exposed than they've ever been thanks to investments in digital infrastructure and the emergence of the hybrid workplace. According to McKinsey, COVID-19 pushed many organizations over a "technology tipping point", forever changing the way they do business. In some cases, it accelerated digital transformation by several years. But while that has helped to make these businesses more efficient and deliver innovative customer and employee experiences, it also significantly increased their digital attack surface. According to one study, 43% of global businesses admit that their digital attack surface is "spiralling out of control". We can see this in:

Cloud computing

Infrastructure-, platform- and software-as-a-service (IaaS, PaaS, SaaS) offer huge IT agility gains and cost benefits. But especially when using IaaS and PaaS, organizations are struggling to secure their environments. The fact that many are managing multiple hybrid clouds only adds to the complexity. Misconfiguration is rife—described as the number one cause of cloud security incidents in 2021. Threat actors regularly scan for exposed systems to compromise.

---

1) A mid-sized business is defined as 50 to 249 employees. A total of 149 mid-sized businesses were surveyed.
2) A large business is defined as 250 employees or more. A total of 134 large businesses were surveyed.

Remote working

Many home systems remain worryingly underprotected. Employees might unduly delay the patching of their corporate laptops or allow the security state of their personal devices to lapse. One 2021 report claims that 45% of IT leaders have seen evidence of compromised printers being used to stage attacks. The home working environment is increasingly seen by cybercriminals as an attractive attack vector for compromising enterprise networks. And now that the hybrid workplace is taking a firmer shape, there may be extra threats from mobile workers connecting via public Wi-Fi hotspots and shared computers.

Home office workers

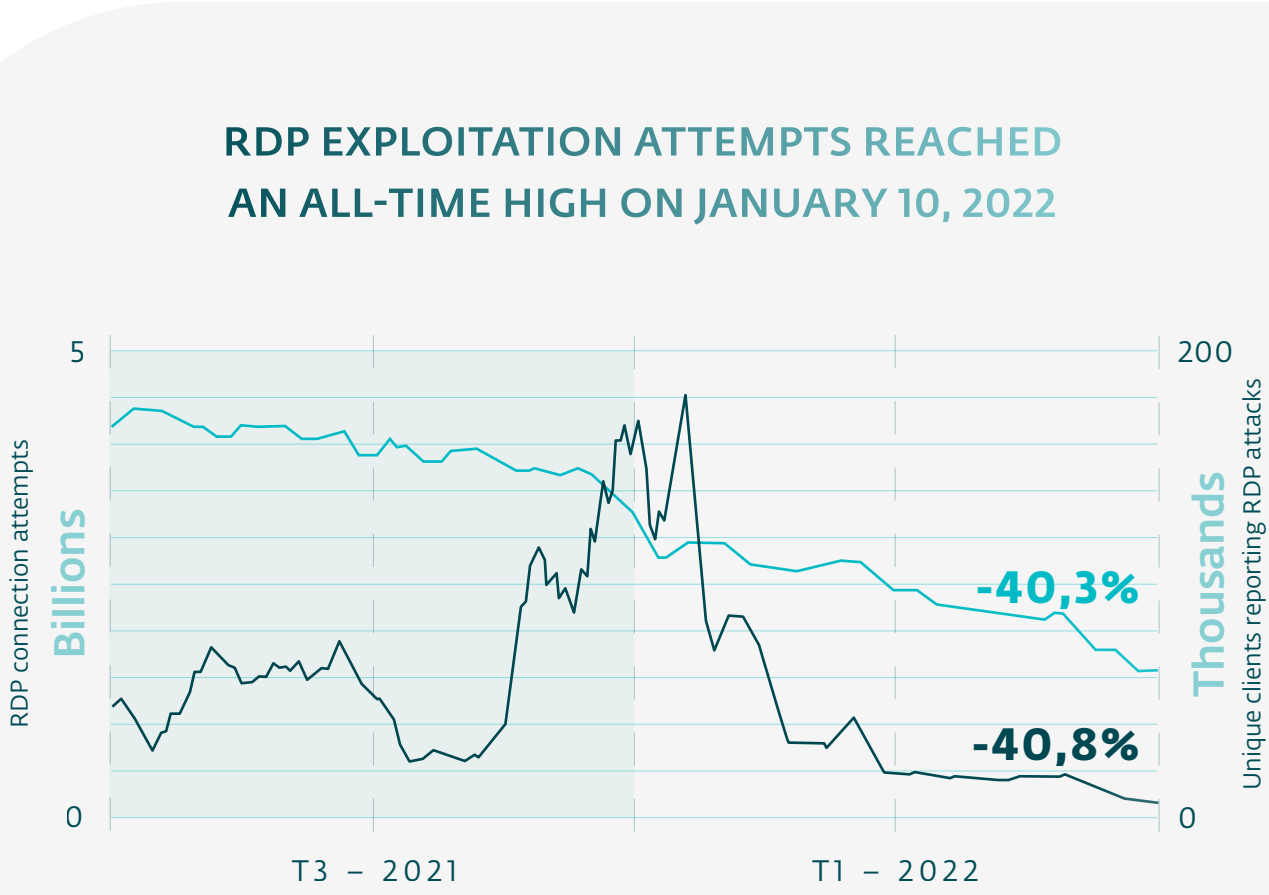
Although remote working devices are often a target for attack, so are their owners. According to Microsoft, 80% of security professionals have encountered increased security threats since the shift to remote work began. And of these, 62% claim phishing campaigns have increased more than any other threat. It's thought that home workers may be more distracted and willing to take risks than their office-bound colleagues, which makes them a perfect target for social engineering. Phishing can be a gateway to ransomware, data breaches, and other forms of compromise. Over a third (35%) of companies say they have seen employees circumventing or disabling security measures.

"Since 2015, there's been a 25% increase in the number of breaches reported, a 500% increase in the number of records breached, and since 2017, a 231% increase in the number of ransomware attacks experienced."

Best Practice: Security Matters, Now What? Forrester Research Inc, May 2, 2022

Remote access infrastructure

The advent of mass remote working also meant a surge in the use of tools like virtual private networks and remote desktop protocol (RDP), which allow for those outside the office to access resources inside. The challenge is that they're often left unpatched or misconfigured. Rather than use multi-factor authentication to further protect access, many RDP accounts are secured with weak or leaked credentials. This enables attackers to quite easily access corporate networks masquerading as legitimate users. RDP is one of the top three attack vectors for ransomware: attempted compromises reached an all-time high of over 4.5 billion[3] on January 10, 2022.



Graph of trends of RDP connection attempts and number of unique clients in T3 2021 – T1 2022, seven-day moving average. source: ESET telemetry)

3) Calculated using a seven-day moving average

Supply chains

This could mean either the physical or digital ecosystems of partners and suppliers. In the physical world, there's a persistent risk of employees and contractors with network access being tricked into giving away their passwords or losing their machines to thieves. In the software supply chain, there's arguably an even greater threat posed by malicious actors tainting the mechanisms and tools used to develop, deploy, and update software with the insertion of malware. IT management software provider Kaseya was compromised by the REvil ransomware group, which leveraged its access to send malicious software updates to the vendor's MSP clients. Over 1000 downstream customers were impacted. Another cause of concern is open-source code that, although commonly used by DevOps teams to accelerate the time to value, can introduce additional risk that is hard to manage amidst complex software dependencies. Over two-fifths (41%) of organizations do not have confidence in the security of the open-source software they use and only 49% claim to have a security policy for its use, according to one report.

49%

of organizations have a security policy that addresses Open Source Software.

Source: State of Open Source Security Report, Snyk, 2022

Threat actors professionalize and innovate

At the same time, the number of threat actors ready to take advantage of these security gaps appears to have surged in recent years. There even exists a ready-made market on which to sell stolen data, buy access and tools, and hire new recruits. Unlike the cybersecurity profession, there appears to be a steady pipeline of talent keen to make a living out of nefarious activities.

We can see innovation everywhere in this cybercrime underground, which is bad news for network defenders. This includes:

1 Ransomware-as-a-service (RaaS)

Just as SaaS popularized software deployment from the cloud, RaaS has made the business of launching and managing ransomware attacks much easier. Affiliate groups can earn up to 80% of the revenue from attacks. In return, they get a starter kit that includes the ransomware payload and attack infrastructure, as well as a breach site to post stolen data on.

Just as SaaS popularized software deployment from the cloud, RaaS has made the business of launching and managing ransomware attacks much easier. Affiliate groups can earn up to 80% of the revenue from attacks. In return, they get a starter kit that includes the ransomware payload and attack infrastructure, as well as a breach site to post stolen data on.

2 Aggressive monetization

Most ransomware attacks today now involve data exfiltration and leakage to force payment. But affiliate groups are increasingly turning the heat up on their victims through a range of additional tactics. These include distributed denial-of-service attacks or contacting customers, partners, and journalists to tell them what's happened. One ransomware group defaces victims' corporate sites to display a ransom note. Another creates bespoke leak sites for each victim, so that customers and employees can check if their data has been exposed.

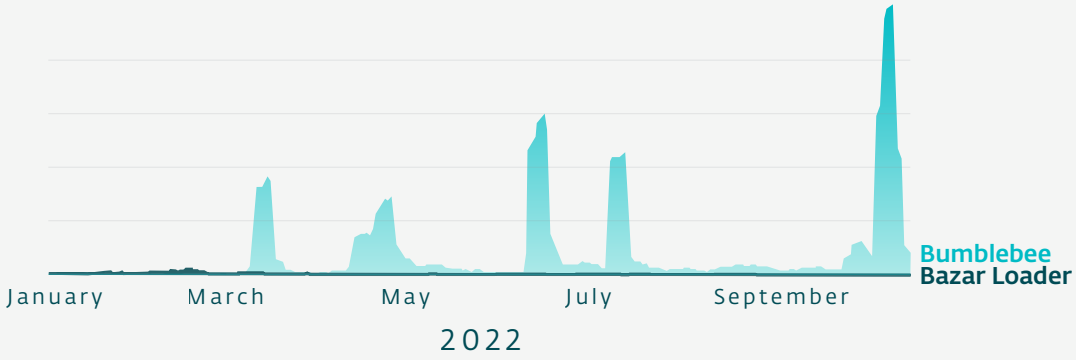
3 Rapid vulnerability exploitation

The number of vulnerabilities tracked in the US National Vulnerability Database (NVD) hit an all-time high in 2021. This makes it increasingly challenging for security administrators to keep on top of the overwhelming number of patches being released. As if that weren't difficult enough, threat groups are becoming increasingly capable of reacting rapidly to zero-day bugs in order to exploit them in attacks. Within days of Microsoft Exchange Server patches being pushed out to fix the ProxyLogon vulnerabilities, as many as 10 APT groups were leveraging them in attacks—hitting over 5,000 Exchange servers in more than 115 countries.

4 The cyberthreat supply chain

The cybercrime underground is increasingly well resourced and professionalized. Specialized groups are emerging to fill specific commercial and operational requirements. For example, when it comes to gaining network access, there's a rise of initial access brokers—experts who compromise targets and then sell this access wholesale to others. One research team spotted a 57% increase in the number of initial access broker listings advertised in cybercriminal forums in 2021 compared to the previous year. Then there is Bumblebee, a loader designed to download and execute additional payloads. It is a successor to TrickBot, a well-known highly resilient beast that survived two takedown attempts in 2020 before being shut down by its operators. For a while, TrickBot's place was claimed by BazarLoader, which was active until the beginning of 2022 but was quickly phased out in favor of Bumblebee. The Bumblebee loader, strongly believed to be operated by the same threat actors as TrickBot and BazarLoader, is active to this day, having launched its latest campaigns in the mid of August 2022.

BUMBLEBEE AND BAZARLOADER DETECTION TRENDS



5 Legitimate tools and fileless malware

Once threat actors get inside target networks, they typically use legitimate tooling and fileless malware to bypass traditional security tools. The idea is to use non-malicious programs to carry out malicious activity such as lateral movement, data exfiltration, process discovery, credential dumping, and arbitrary command shell execution. These programs include PowerShell, PsExec, and Cobalt Strike.

6 Advances in phishing and social engineering

Sometimes the old ways are the most effective. Phishing still represents one of the top three attack vectors for ransomware, even hitting a record high in Q1 2022. The bad guys keep on tweaking their techniques to stay one step ahead of email filters and security training programs. Among the most popular is email thread hijacking, whereby attackers compromise an inbox and then hijack existing conversations in order to disseminate phishing links. Because a reply message appears more genuine than unsolicited one, any links included are more likely to be clicked. Another technique is smishing (SMS phishing), which bets on users being more distracted when looking at their smartphone screens, and therefore more likely to click through. One vendor recorded a doubling of smishing attempts in the US during 2021 and over 500 thread hijacking campaigns the same year, linked to 16 different malware families.

From prevention to XDR

Ransomware is certainly where a lot of cybercrime innovation is happening. According to British government security experts, this has propelled ransomware to become the number one cyber risk for organizations. It's easy to see why when one group alone (Conti) managed to compromise at least 859 organizations in just two years—including 40 in only a month—and make billions in cryptocurrency in the process. According to one estimate, ransomware detections soared 148% year-on-year to reach 470 million in the first three quarters of 2021, making it the worst year on record.

But ransomware is far from the only threat to global organizations today. Data theft, cryptomining malware, banking trojans, and spyware, among others, are all jostling for a seat at the table.

The cumulative impact of these trends should focus IT security leaders on an inescapable truth. **Threat prevention should always be preferred, but sometimes it's not possible**. There are simply too many ways for bad actors to get into the corporate environment unseen. That's why organizations should balance prevention with detection and response. This is what ESET's Prevention, Detection and Response (EPDR) approach focused on, by blending multiple layers of security technology. First, it aims to protect by blocking malicious code or actors from entering or damaging a user's system. But if that fails, there is powerful detection and response to mitigate advanced threats that manage to compromise a system.

Think of it as locking and bolting all your doors and windows, but then installing motion detection alarms to catch suspicious activity if anyone does make it inside the house. XDR is a key asset here. It enables security operations (SecOps) teams to gain unparalleled visibility into their IT environment from a single pane of glass and spot anomalies indicating threats via high-fidelity alerts. XDR[5] is an evolution of EDR, which optimizes threat detection, investigation, response, and hunting in real time.

---

5) Definition of XDR by Forrester, 2021

XDR unifies security-relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management, cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation.

XDR enables you to answer several key questions about a cyberattack:

- **How did it start?**
- **Where did it start?**
- **When did it start?**
- **Which endpoints are infected?**
- **Is it contained?**
- **How do we prevent it in the future?**

Most importantly, it can help you take rapid remedial action to resolve incidents before they severely impact the organization.

How can MDR help?

However, even with the help of XDR, SecOps teams face major challenges from an organizational perspective. Many of these, especially a lack of in-house knowledge, expertise and resources, are particularly pronounced among SMBs. The overall challenges for organizations include:

Talent shortages

The cybersecurity industry has a current shortfall of 2.7 million workers, and security operations center (SOC) analysts are arguably among the hardest to come by and retain. The problem is worsened by the impending plans of many analysts to quit in 2023 due to the stress and burnout associated with alert overload. IT generalists often can't dedicate several hours in a day to man an XDR solution. The challenge is most acute among SMBs, which generally lack the in-house knowledge and expertise needed to man a SOC and could thus benefit most from MDR.

Costs

It's not just the cost of hiring and retaining talent to man the SOC that security leaders need to think about. They must also find the right blend of tools to provide the insight their analysts need. This can cost a significant outlay up front, and in ongoing license fees afterward.

The financial burden on organizations that choose to do SecOps in-house is growing. According to one study, the perceived return on investment is dropping in over half of organizations due to management complexity. The same report claims security engineering costs are creeping toward US$3 million annually, but only 51% rate these efforts as effective.

Security gaps

Tooling is sometimes not up to par. This can lead to alert overload and subsequent alert fatigue. If SOC staff are overwhelmed by false positives, they may end up spending hours chasing dead ends while legitimate signals are missed. When multiple tools are feeding into the SOC, this can also create coverage gaps.

Management

Getting products procured, installed, and correctly configured are just the first steps. Managing multiple SOC tools and analysts across multiple jurisdictions can be a significant challenge. When resources are already stretched to the limit, important tasks are sometimes missed. It's easy to be run down by fighting incoming threats and losing the time to reflect and plan strategically.

There's a perception that enterprise IT security teams want and are fully able to tackle these fast-evolving challenges—that they fully understand the software they purchase and are forming mature in-house SOCs to face down cyberthreats. In fact, research conducted by ESET[4] shows that:

68% **of enterprises prefer their security vendor to deploy security products**

75% **expect their security vendor to offer cybersecurity issues support, consultation, and incident response**

87% **want 24/7/365 cybersecurity support services**

90% **want vendors to provide threat monitoring, hunting, response, and remediation services**

4) Internal ESET Research Survey among 404 Enterprise-grade respondents.

What are the key benefits of MDR?

This is where MDR can bring tremendous benefits for organizations that want to mitigate cyber risk, but don't have the in-house resources to do so effectively. Although MDR may vary from provider to provider, it should include at least some variation of the following:

Threat detection

Threat actors have countless ways to sneak through perimeter defences. But by leveraging behavioural analytics, they can be spotted early on so that organizations can take action to resolve attacks. Proactive threat hunting can also be used to look for sophisticated attacks that may be able to evade automated checks.

Prioritization

Intelligent analytics generate context, which allows MDR systems to turn data into actionable information and flag alerts with higher fidelity. This is a critical phase of the MDR workflow given how many SOC teams struggle with alert overload.

"MDR services already address much of what XDR aspires to do. MDR delivers better security outcomes by providing tools and technologies such as threat intelligence, threat hunting, 24 x 7 consistent monitoring, advanced analytics, and containment and removal of incidents or breaches where data is suspected or known to have been exfiltrated or destroyed. IDC believes that an MDR offering should go beyond offering guidance and recommendations."

Source: IDC Global Security Products Analysis: From Power Point to Power Product, Where Is XDR Right Now?, Doc # US47705821, February 8, 2022, Ch. Kissel, M. Suby, F. Dickson

Analysis

Automated behavioural analysis combines with human assessment to investigate whether an alert is a true positive and what steps need to be taken to resolve an issue.

Response

Thanks to the previous analysis phase, the system will understand what kind of response is required to contain and eliminate the threat and remediate any compromised systems. This could entail a password reset, patching specific endpoints, or even reimaging computers.

The benefits of outsourcing detection and response are simple but compelling:

- The MDR provider takes care of all management of the back-end technology, freeing up staff to focus on high-value, strategic tasks rather than drowning in alerts
- The MDR provider may also optimize and manage the back-end technology to align with each customer's risk profile and infrastructure
- With detection and response managed by a third party, there will be no need to pay hefty salaries to attract and retain the best SOC talent
- Customers can benefit from their provider's economies of scale, ability to attract the best talent, and insight into other customer organizations and threat environments

WHAT TO LOOK FOR IN AN MDR SOLUTION?

With so many MDR solutions flooding the market, it can be challenging knowing where to start. Consider a provider capable of offering at least the following:

Research excellence:
Best-in-class intelligence built on industry-leading research capabilities.

High quality customer service:
Including hyperlocal language support combined with global presence and delivery.

Customization:
A made-to-measure solution personalized for each customer's size, IT complexity, and required level of protection.

Leading detection and response capabilities:
Independently tested to become products renowned for their high detection rates, low false positives, and light footprint.

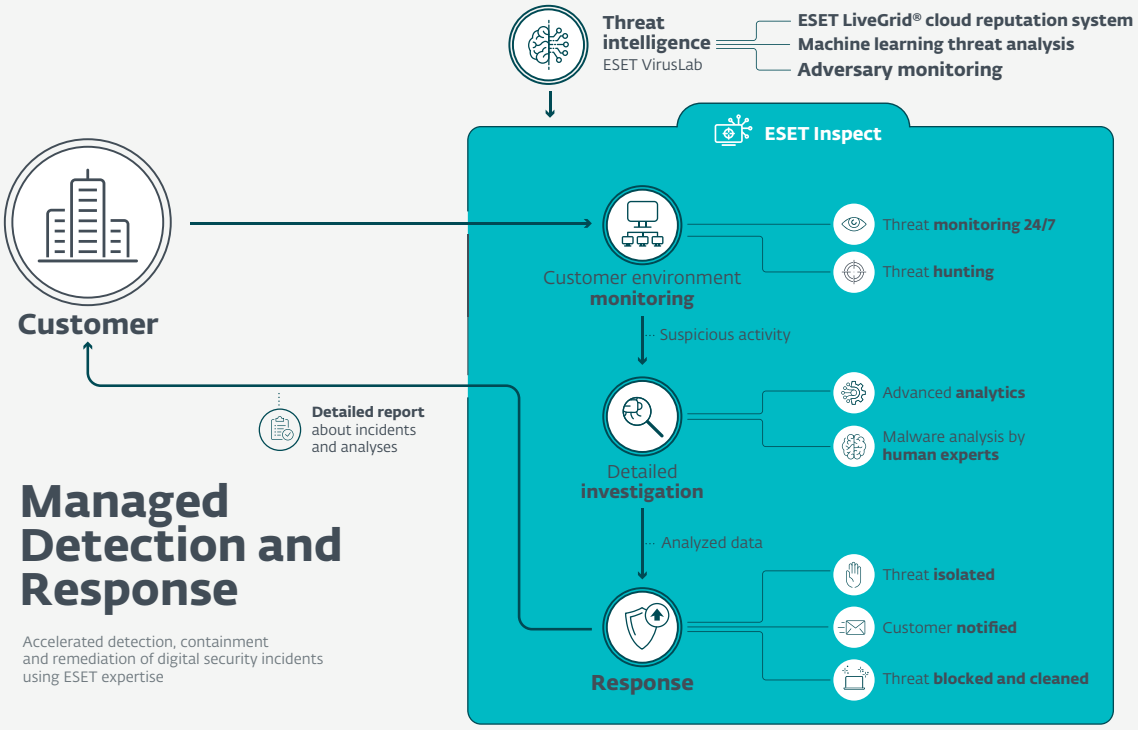
Cyber-threat hunting:
Expert analysts use advanced tooling and their own expertise to proactively search for sophisticated threats that may be hiding undetected in the network.

24/7/365 operations: Threat actors operate from around the globe and in multiple time zones, so any service must be on high alert round the clock.

HOW ESET CAN HELP WITH MDR

ESET's MDR capabilities combine **industry-leading technology** solutions, including XDR, with world-class security research and threat intelligence built on more than **30 years of expertise**. The result is an enterprise-class SOC equipped with the tools to leverage our **groundbreaking research** on malware, social engineering, obfuscation techniques, APT groups, and much more.

But this is no one-size-fits-all service. Each engagement begins with an assessment of the customer's environment, infrastructure, organizational composition, and general cybersecurity culture. This helps us to create an **individual customer security profile** and allows us to act as a seamless extension of your IT security function. In fact, ESET has significant experience **protecting clients across all sectors** – and specialized expertise in a range of industries and verticals. Using ESET technology allows customers to leverage that experience.



ESET MDR service, ESET Detection and Response Ultimate provides a complete, multiregional product and services suite delivering:

- **A team of cybersecurity experts** ready to handle deployment, optimization, daily monitoring, periodic threat hunting, malware analysis, and incident response for a broad range of organization sizes. Local teams work closely together with the global threat intelligence team, which sits at the beating heart of MDR and our other managed services.
- **30+ years of own malware research** gives us the expertise to monitor customer environments for advanced threats and breaches. And we have experts behind our internationally acknowledged research, shared via WeLiveSecurity, delivering the service.
- **Incident investigation and response**, including basic and detailed file analysis, reverse engineering, digital forensics, and incident response assistance
- **A local presence with global scale** delivered by a large network of partners, regional offices, and several expert malware research teams at ESET headquarters and across the globe.
- **Endpoint security support assistance** to tackle missing malware detections, cleaning problems, investigation of suspicious behaviour, and to mitigate ransomware attacks
- **ESET Inspect support** to help with any questions that might arise about our XDR tool, such as help with creating custom rules and exclusions
- **Daily threat monitoring** available 24/7/365 to ensure the environment is clean and permanently protected, and that threats are detected as early as possible
- **Proactive threat hunting** once every three months by default to ensure the environment remains protected from the latest threats. These investigations leverage ESET's expansive knowledge of indicators of compromise and potential threats pointed out by customers

Monthly reporting is the result of our monitoring and service delivery. It also contains Security Advisories from our Security Analysts. In the reports we created over the years we see the number of detections and incidents lower over time as customers follow up on these Advisories. These are not only ESET product and configuration-related but contain actionable advice on the type of activity we see within the environment like Brute Force detections or phishing, and the specific users who tend to click on these.

ESET MDR service (Detection and Response Ultimate) as a holistic solution can be purchased as part of the ESET PROTECT MDR offering. This is a more comprehensive option combining products and services covering prevention, detection, and response. Managed via a single pane of glass, these include:

- Management Console (ESET PROTECT)
- Endpoint Protection Platform (ESET Endpoint Security)
- File Server Security (ESET Server Security)
- Advanced Threat Defense (ESET LiveGuard Advanced)
- Full Disk Encryption (ESET Full Disk Encryption)
- Extended Detection & Response (ESET Inspect)
- MDR Service (ESET Detection and Response Ultimate)
- Premium Support Service (ESET Premium Support Advanced)

WHAT DOES A SUCCESSFUL MDR DEPLOYMENT LOOK LIKE?

THE CASE OF ROYAL SWINKELS BREWERY

Royal Swinkels, the second largest brewery in the Netherlands making over 300 beers in more than eight breweries all over the world and sold in more than 130 countries, share their experience with deploying MDR from ESET. Making beer these days is a highly automated process depending on IT and OT (industry automation). A breach or negative event could mean a disruption in supply chain and have a heavy impact on deliveries and revenue. MDR from ESET helps them protect against such risks. The ESET team manages the detections and response, filter all the alerts, monitor environment, as a 24/7 service of qualified IT security staff.

"Every company of our size is heavily reliant on IT these days. On the one hand we are not big enough to have our own Security Operations Center, but on the other hand we are not that small that we can just wait until something happens. we didn't like that reactive approach, so we've chosen proactive approach and that's why we chosen MDR, so that we can put the management to ESET. "

Robert Heines,
Royal Swinkels Family Brewers

To find out more about how ESET can support your journey to enhanced prevention, detection, and response, check out our resources on ESET PROTECT MDR and extended detection and response.

CONCLUSION

Security decision makers face a challenging period of converging trends. Following the years of global crisis,, the corporate digital attack surface has expanded significantly. At the same time, threat actors are increasingly emboldened, determined, and well resourced. Security operations managers are struggling to deflect more sophisticated attacks when teams are stretched to the limit, point solutions are underpowered, and resources remain scarce. Funding a fully-fledged 24/7/365 SOC in this context is beyond all but the largest enterprises.

Breaches are inevitable, but they don't have to result in serious financial and reputational damage if adversaries can be found and incidents resolved at speed. MDR was made for this. It hands off the heavy lifting to a dedicated provider, minimizing security risk for the customer organization while freeing staff to work on high-value tasks and revenue to spend strategically elsewhere.

"Service providers can deploy MDR services utilizing a mixture of clients' existing capabilities, cybersecurity partners' supplied tools or services, and private intellectual property. This partnership forms a powerful combination of advanced EDR/extended detection response (XDR) solutions, human expertise, threat intelligence, threat hunting, enhanced consoles, dashboarding and reporting, and various forms of intellectual property developed by the MDR service provider."

Source: IDC, The Evolution of Managed Security Services, Doc # US48459521, December 2021, P. D. Harris, CISSP, CCSK

Independence, integrity, innovation, expertise: these are the foundations on which ESET builds its award-winning cybersecurity solutions.

With ESET, your organization can benefit from:

- A made-to-measure solution customized to fit your size, IT complexity, and required level of protection
- Complete coverage from ESET cybersecurity experts acting as silent partners
- Peace of mind that any sensitive information shared will be handled by a trusted partner
- Hyperlocal language support in many countries
- Research excellence built on 30 years of cybersecurity expertise
- Built-in ransomware assistance, malware analysis, digital forensics, and incident response at no extra cost
- Industry-leading endpoint security optimized for performance while offering a strong detection capability
- A malware research team providing decades of expertise to mitigate customer skills shortages

LEARN MORE ABOUT ESET PROTECT MDR

ABOUT ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide.

ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

ESET IN NUMBERS

1bn+
internet users protected

400k+
business customers

200+
countries & territories

13
global R&D centers

RELY ON A GLOBAL TECHNOLOGY LEADER TO PROTECT YOUR ENTERPRISE