MDR + IR

A Recipe for Cyber Resilience in a Twenty-First Century Risk Landscape

I. Introduction: Today's Challenging Threat Landscape

The more things change, the more they stay the same. Although the events of 2020 initiated profound change within many organizations' technology environments, many of the threats that security leaders continue to face are very familiar. The same threat actions that resulted in the greatest number of data breaches in the past are just as prevalent as ever. A majority of the past year's breaches (59%) involved phishing, the use of stolen credentials or privilege misuse.[1]

However, nation state-sponsored cyberattacks have grown in frequency and sophistication, with commercial enterprises now their most common target.[2] Ransomware attack volumes have also skyrocketed, and the average ransom payment demand climbed to a historical high of $847,344 in 2020.[3]

At the same time, IT environments continue to grow in complexity as consumer demand for digital services increases. Businesses across industries have no choice but to store and handle swelling volumes of customer and employee data, electronic health records, priceless intellectual property and other information assets. It's simply impossible to remain competitive without digitizing more and more areas of the business. Yet each new online service, addline of code, or recently introduced technology, has the potential to increase cybersecurity risks.

This brings us to a situation where it's become impossible to avoid cyber risk. There is no end in sight.

No matter how strong your safeguards, how powerful or cutting-edge your technologies, or how robust your processes, cyber defenses can — and will — fail. Even with the best security awareness training programs in place, employees remain humanly fallible, and a single click on a phishing email or hasty response to a carefully crafted social engineering scheme is all it will take. Whereas defenders must continue to block threat after threat and thwart attack after attack with unending vigilance, threat actors only have to succeed once.

The Prudent Approach to Risk Management

Today's Chief Information Security Officers (CISOs) are increasingly adopting an "assume breached" mentality. This includes creating robust security monitoring capabilities which enable teams to rapidly detect, respond to and contain any cyber threat with the potential to disrupt the business. For small and midsized organizations without the resources to build, staff and maintain an in-house 24/7 Security Operations Center (SOC) — a time-consuming and labor-intensive process costing millions of dollars a year — relying on a trusted partner to deliver these capabilities has become essential.

[1] https://enterprise.verizon.com/resources/reports/2020/2020-data-breach-investigations-report.pdf, [2] https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf, [3] https://start.paloaltonetworks.com/unit-42-ransomware-threat-report

Managed Detection and Response (MDR) services continue to gain market share as growing numbers of business leaders realize that leading MDR providers are able to maintain more comprehensive threat visibility across today's varied and dynamic IT environments than legacy Managed Security Service Providers (MSSPs) could, while also aiding with incident containment and remediation efforts. All too often, traditional MSSPs function as a mere alert factory, delivering high volumes of false positives without an actionable response component to their services. MDR instead delivers real-time response, conducted by an expert professional, to quickly and effectively contain threats that evade endpoint agents and dodge network-based defenses.

This eBook examines why it's now necessary to augment MDR services with Incident Response and Digital Forensics capabilities. In today's world, organizations need what MDR delivers – the capacity to perform threat containment and remediation in case of an incident. But they also need to extend their capabilities further into the incident response lifecycle. As advanced and highly targeted cybercriminal activities become more and more common, they must be able to perform full-scale cyber investigations whose results will stand up in a court of law.

Do you have the expertise you need to hunt out, investigate and respond to every threat?

II. MDR Services: Balancing Technologies and Human Security Expertise to Close the Gaps

Nearly all of today's businesses face significant degrees of operational cyber risk. As large-scale, high-profile breaches make headlines over and over again, there's growing awareness among key business stakeholders about the nature and extent of this risk. There's also increased understanding of other key factors that are driving businesses to engage MDR providers. These include:

- the cybersecurity skills gap
- the severity and sophistication of present-day threats
- the complexity of modern IT ecosystems
- the imperative to secure remote and hybrid workforces

According to analyst firm Gartner, as many as 50% of organizations will use MDR services for threat monitoring, detection, response and containment by 2025.[4]

However, choosing the right provider can be challenging in what has become a crowded and noisy marketplace. When Gartner first began tracking this segment in late 2016, only 14 companies were identified as representative vendors. Today, well over a hundred providers claim to be offering MDR services.

[4]https://www.gartner.com/doc/reprints?id=1-248Q18GC&ct=200925&st=sb

Look for an MDR provider who can cover major areas of operational risk:

Your Risk	Poor visibility and blind spots	Unknown threats establish persistent present in your network	False positives that extend attacker dwell times	Taxing your internal resources	Excessive costs
Provider's Capabilities	Adequate coverage of your entire attack surface, including endpoints, network and cloud	Ingesting and processing security data at scale, and leveraging automated analysis and expert human investigations	Marrying world-class SOC analysts with advanced technologies to enable rapid, precise identification of threats	Full-scale threat hunting and response capabilities across the entirety of the incident lifecycle	Effective real-work risk mitigation coupled with effective response capabilities that contain attackers quickly

Engaging with a quality MDR provider means that you can expect to attain comprehensive visibility across your environment, which translates into rapid threat detection. The provider should be ingesting multiple signal sources, which translates into superior investigative and data correlation abilities. You will also have an active threat hunting program, which translates into the ability to be proactive. And you will have remote containment capabilities, which translates into accelerated responses and reduced attacker dwell times. Taken together, these capabilities will support the adoption of a Zero Trust approach to information security. You'll no longer need to guess about whether or not attack surfaces are exposed, vulnerabilities are present, or an undetected compromise has occurred.

Core capabilities of an industry leading MDR provider

- Multi-signal visibility
- Machine learning-driven Extended Detection and Response (XDR) capabilities that eliminate noise and automate threat detection and disruption
- 24/7 threat hunting with human-led investigation
- Rapid response including threat isolation and containment
- Remediation and recovery support
- Risk management recommendations

III. Extend Capabilities Across the Full Incident Lifecycle with Incident Response and Digital Forensics

The right MDR provider will supply you with capable and full-featured security monitoring coverage, as well as elite threat hunting, alerting, triage capabilities, remediation recommendations, tactical threat containment, and remediation verification. In some service agreements, co-remediation or deeper response capabilities are also included.

While MDR gives you access to 24/7 expert SOC support, these services weren't specifically designed to furnish evidence that will serve in a court of law. If you need to conclusively determine the precise extent of data loss, or you're looking to investigate an incident in granular detail – right down to the level of the individual compromised record – you'll need to call in a specialist.

Incident Response and Digital Forensics Services provide much deeper cyber investigative capabilities. Grounded in the underlying science of digital forensics, this is a distinct discipline that incorporates evidence handling techniques as well as the mastery of digital forensics tools. It is explicitly designed to fulfill the most exacting requirements of cyber insurers, regulators and prosecutors.

MDR vs. Incident Response and Digital Forensics

	MDR	Both	Incident Response and Digital Forensics
Empower organizations to respond systematically to early-stage attacks	✖		
Identify and fill gaps in defenses	✖		
Handle ~80% of events, incidents and minor breaches	✖		
Minimize loss or theft of information		✖	
Limit disruption and damage		✖	
Ensure incidents are handled consistently		✖	
Recover from business-altering incidents			✖
Comply with legal and regulatory post-breach requirements			✖
Cover the most severe incidents (those that fall out of scope of MDR services)			✖

Three key reasons you need ongoing access to cyber security investigation capabilities:

1. **Cyber insurance:** Insurers typically require covered entities to adhere to industry standard cybersecurity best practices. Increasingly, this means companies must establish and maintain a retainer agreement with an Incident Response provider with extensive digital forensics capabilities.
2. **Regulators:** A growing number of formal regulatory frameworks as well as those that are not mandatory to adhere to but are generally taken to delineate best practices across multiple industries (such as the National Institute for Standards and Technology (NIST) Cybersecurity Framework), specifically mention that IR capabilities must be in place. To satisfy today's regulators, it's necessary to have more than just an incident response plan.
3. **Legal evidence:** It's impossible to predict when your organization might be victimized by nation state-level attackers, organized criminals or cyberterrorists. But if this situation ever comes to pass, you may be obligated to provide digital evidence in a court of law. You might also need to furnish digital evidence in case there is litigation and you're accused of failing to meet industry best-practice standards. Or you may face a legal obligation to notify individuals in the event their personal data was compromised. It's critical to understand the exact scope of such incidents and have the right evidence on hand.

IV. Benefits of Converging MDR and IR

Streamlined workflows

The biggest benefit of working with a single provider with converged MDR and IR capabilities is that you gain time to value in expert level response across the entire incident lifecycle. Combining 24/7 SOC service with incident responder capabilities amplifies the support of hundreds of professionals who are already accustomed to working together at a high level. Investigation, containment and recovery efforts can be collaborative and driven around-the-clock. Bear in mind that your MDR team will already be familiar with your environment, understand which logs you are collecting and know which security tools you have in place. This provides a major advantage in a high-pressure evidence-handling operation. Your MDR team can turn over the cyber incident investigation to digital forensics experts that they know well and are accustomed to working with, developing streamlined processes that will serve as a force multiplier in real-world attacks.

When push comes to shove and investigative actions are needed to drive decision making and produce evidence that could bear scrutiny in a court of law, no one is better positioned to respond more meaningfully and impactfully than your MDR provider. It takes more time to hand off to a third-party provider, and you could suffer a loss of knowledge and expertise in the process of the transfer as well. When you combine the capabilities of an elite threat hunting team, incident responders within the SOC and a specialized digital forensics and IR team, you get better, faster and more accurate containment, evidence handling, remediation and root cause analysis.

Know who to turn to in the moment of crisis

Organizations without a pre-existing IR retainer agreement in place at the time of a breach will be challenged to evaluate potential providers at a moment when time is of the essence and when business leaders and technical team members alike will face high emotions and tough choices. It's hard to make a wise, evidence-based decision at this point.

Furthermore, the faster you can respond, the more likely you are to reduce damage, mitigate costs and gather valuable evidence before attackers can destroy it. A team that's already working within your environment has a massive advantage when it comes to taking action at speed.

Alleviate the burden on your team

An expert IR provider will already have helped you build an incident response plan. This should be developed at the beginning of the engagement, and will include steps for handling crisis communications, public relations, legal obligations and breach notifications (if they are indeed necessary). This plan's development will have been guided by an industry expert who thoroughly understands whom you must inform (such as customers, regulators and your insurer), when and how.

With a comprehensive end-to-end detection and response process established across the whole of the incident lifecycle, your internal security team can focus on the areas where they're able to contribute the most value instead of worrying about "what ifs."

Take a deeper dive into incident response and digital forensics to understand why your business needs these capabilities in the current cyber threat landscape.

V. The Value of Digital Forensics and Asset Handling Expertise

Risk management is a core component of the strategic business planning that any enterprise must do. In the current threat landscape, cybersecurity risks are omnipresent, severe and have the potential to destroy a business. It is crucial that these risks be managed strategically.

Regardless of the strength of your defenses, it is simply impossible to mitigate or avoid all types of cybersecurity risk. Maintaining digital forensics capabilities is a critical means of managing the legal and reputational risks that your business carries due to its dependence on technology and the nature of today's world.

Unavoidable Cyber Risks

Infrastructure risks: The average organization runs more than 450 different software applications and gives 182 partners and vendors some type of access to its IT environment on a weekly basis.[5] Digital supply chain-based breaches like the recent compromise of the SolarWinds IT monitoring and management software or the Microsoft Exchange Server hack remind us that these risks are unavoidable in a world where tool standardization and connectivity are necessary for doing business.

Industry-centric risks: It's simply impossible to avoid the risks that are inherent to operating in your industry. For instance, electronic health records (EHR) are an attractive target for threat actors due to the high values they fetch on the black market. No healthcare organization can eliminate these risks.

Human-centric risks: No matter how careful or well-intentioned they may be, people make mistakes. And the possible existence of insider threats cannot be eliminated.

[5]https://www.beyondtrust.com/assets/documents/Privileged-Access-Threat-Report-2019.pdf,

Because all cyber risk cannot be mitigated, exercising due diligence means you must be able to demonstrate that you did what any reasonable person would do to balance these risks. Increasingly, insurers, regulators and courts expect that organizations will have IR capabilities in-house or will maintain these capabilities through a retainer agreement. Such expectations are only becoming more commonplace as these services become more widely available. Cybersecurity insurance policies, in particular, are changing in the face of the current devastating global ransomware epidemic. Carriers are increasingly requiring companies to plan and prepare for incident mitigation and response and are becoming less willing to reimburse ransom payments.[6]

Nonetheless, it remains challenging and expensive to recruit employees with the right qualifications and expertise. Incident response is a highly specialized field with multiple subdomains including forensics, incident handling and intrusion investigation. It's critical to ensure that digital evidence is collected according to specific procedures that protect it from tampering or contamination. As part of the chain of custody, you must be able to prove in a court of law that this has been achieved. Incident response professionals must also be highly skilled in translating their findings into terms that law enforcement and legal professionals will understand. Finally, they must be able to deliver a battle-tested response to real-world cyberattacks – even under the industry's most stressful conditions.

> When an incident takes place, it's critical to have a team of experienced individuals. They need confidence, experience, and first responder-type personalities. They need to be the people who will run into the fire rather than away from it. This requires extensive training, but also a certain emotional tenor.
>
> - Mark Sangster,
> *Principal Evangelist and Vice President of Industry Security Strategies, eSentire*

VI. What Can Happen Without IR Expertise in Place

It's all too common for well-intentioned managed service providers (MSPs) to destroy the evidence.

It happens all the time when there's a ransomware attack... an IT technician will remove the affected hard drive, discard it, and restore from a backup. But once this process is complete, you've lost all digital forensic evidence, and along with it, the possibility of claiming valuable legal recourse. You may also have rendered your organization negligent. And you've made it more difficult to figure out how to remediate the vulnerability that led to the attack in the first place.

[6] https://abcnews.go.com/Technology/wireStory/insurer-axa-halts-ransomware-crime-reimbursement-france-77540351#:~:text=BOSTON%20%2D%2D%20In%20an%20apparent,payments%20made%20to%20ransomware%2-0criminals.&text=That%20helped%20drive%20ransom%20payments,average%20of%20more%20than%20%24300%2C000

Moving too slowly can result in significant financial losses and reputational harm.

The average data breach in 2020 cost its victim a total of $3.86 million and took 280 days to fully identify and remediate but organizations able to move more quickly are spared a considerable portion of these expenses. Those with both IR teams and fully tested IR plans in place saved an average of $2 million in breach costs,[7] while also limiting their legal liability and minimizing reputational damage.

When a company has both MDR and IR capabilities on hand, the time savings they'll experience in case of an incident are significant. Leveraging an engagement model that converges Incident Response with Threat Intelligence, 24/7 SOC Analyst Expertise and advanced network and endpoint sensor technology can greatly accelerate time to value for both threat suppression and complete incident resolution. Industry-leading providers have recently revolutionized incident response times, making a four-hour threat suppression service-level agreement possible. And these rapid response times – which far surpass the industry average – can be achieved remotely, anywhere in the world.

Many organizations suffer avoidable harm because of misunderstanding regulatory or contractual obligations.

The reputational damage that a company undergoes in the aftermath of reporting a breach can be crippling. The average breach victim in 2020 lost $1.52 million in revenues due to increased customer churn and greater cost of acquiring new customers.[8] Many organizations, however, suffer needlessly, reporting as a "breach" something that actually should have been classified as an "incident." In a number of cases, what took place did not in fact meet the legal and contractual requirements for something that should have been reported at all.

Action Plan: What to Do if You've Suffered a Breach

- Follow your incident response plan to the letter, documenting how you've done so
- Set up a war room
- Call in the teams (including legal, PR, executive and technical) that you've designated to handle the situation
- Scope the incident thoroughly before deciding on a plan of action or communications
- Tap into your partner ecosystem if you don't already have an IR provider on retainer
- Don't overspend on technology in the wake of the incident
- Gain value from lessons learned and refresh your incident response plan accordingly

[7]https://www.ibm.com/downloads/cas/RZAX14GX,[8]https://www.ibm.com/downloads/cas/RZAX14GX

VIII. What to Look for in an IR Provider

Having a full-scale, professional incident response and cyber security investigations team on hand whenever you need them gives you access to capabilities that MDR engagements alone won't provide. These include:

In case of emergency:

- Rapid mobilization and deployment aimed at quickly securing your systems and networks
- End-to-End Incident Management
- Digital Forensic Analysis collecting as much information and insight as possible from your systems and networks
- Regression analysis to conclusively determine the full extent of compromised assets and determine root cause
- Stakeholder Reporting
- Compliance support to meet regulatory requirements with centralized collection, retention and reports of log, network and endpoint data
- Litigation Support as required
- Crisis Communication Support

On an ongoing basis:

Incident Response Retainer

- Many providers will have dedicated hours available for Emergency Incident Response and additional Incident Response Strategic Services
- Service Level Agreements (SLAs) should be expected for threat suppression, onsite support and malware analysis

Sample Security Consulting & Advisory Services

- Data discovery and classification
- Managed data loss prevention
- Managed insider threat programs
- Risk-based security management

Sample Security Incident Response Planning (SIRP)

- Incident Response Life Cycle Planning
- Incident Response Policy Development

Sample Simulations and Training

- Cyber wargames
- Tabletop exercises
- Compromise assessment

5 Key Questions to Ask a Potential IR Provider

1. ***What IR services does our organization need?*** The right provider for your organization is one who takes the time to thoroughly understand your environment and needs. A provider who begins with a consultative approach will be able to help you identify functional gaps and make you aware of things you might otherwise have overlooked.

2. ***What are your qualifications?*** Because Incident Response is a highly specialized field, potential providers should be ready, willing, and able to provide you with a list of certifications.

3. ***Have you worked with other clients in our industry or field?*** Because regulatory requirements are industry and geography-specific, it's crucial that the provider understand the laws governing your activities. It's also important that they be familiar with the tools and technologies commonly employed in your industry, and that they understand your customers' expectations and contractual obligations. These are vital facets of your operational context that inform your risk profile and how you should ready yourself to respond to incidents.

4. ***How will you work together with our internal team?*** It's important that both parties understand what the nature of the working relationship will be. Ideally, your team should work together with your chosen provider to develop policies, plans and procedures.

5. ***What related services do you offer?*** There are many proactive and reactive services related to IR that go beyond those activities immediately defined as Incident Response, and there is considerable benefit to finding partners who can offer such services. Doing so reduces the number of third parties involved, avoids complications when it comes to information sharing and accelerates response times.

Conclusion

Today's cybersecurity risks can neither be completely mitigated nor entirely avoided. A data breach or significant incident can result in lasting reputational damage, major operational disruption and significant legal and regulatory repercussions. While full-scale MDR services bring enhanced visibility, rapid threat detection and the ability to respond to and remediate early-stage attacks, their effectiveness can be enhanced with the addition of incident response and digital forensics capabilities.

Why Organizations Choose eSentire

eSentire is recognized globally as the Authority in Managed Detection and Response services because we hunt, investigate and stop known and unknown cyber threats before they disrupt your business. We were founded in 2001 to secure the environments of the world's most targeted industry - financial services. Over the last two decades we have scaled our cybersecurity services offering to hunt and disrupt threats across every industry on a global scale. With two 24/7 Security Operations Centers, hundreds of cyber experts, and 1500+ customers across 80+ countries, we have demonstrated the ability to Own the R in MDR with a Mean Time to Contain of 15 minutes. While many cybersecurity companies focus on detection, we recognize that there is no end to cyber risk. Preventative technologies will be bypassed, and defenses will fail. That's why eSentire prioritizes Response.

We deliver MDR³ - Response. Remediation. Results.

We deliver cyber program results through a combination of cutting-edge machine learning XDR technology, 24/7 threat hunting expertise and security operations leadership. eSentire offers comprehensive security services to support your business operations end-to-end as we stop breaches, simplify security and minimize your business risk:

Managed Risk Services
Strategic services including Security Assessments, Managed Phishing and Security Awareness Training, and Managed Vulnerability Services to identify gaps, build defensive strategies, operationalize risk mitigation and continuously advance your security program.

Managed Detection and Response Services
We deliver complete and robust Response. By combining cutting-edge machine learning XDR, human security expertise and security operations leadership, we hunt and disrupt known & unknown threats before they impact your business.

Digital Forensics and Incident Response Services
Battle-tested Incident Commander level expertise driving incident response, remediation, recovery, and root cause analysis. Emergency Preparedness and Emergency Response services as well as industry-leading 4-hour Threat Suppression SLA with eSentire IR Retainer available.

$6.5T+
Total ALUM

1500+
Customers in 80+ Countries

20.5M
Daily Signals Ingested

3M
Daily Atlas XDR Automated Disruptions

6000
Daily Human-led Investigations

700
Daily Escalations

400
Daily Threat Containments

15min
Mean Time to Contain

Awarded

IDC LEADER

CYBER SECURITY EXCELLENCE AWARDS WINNER 2021

MSSP Alert TOP 250 MSSPs 2021 EDITION NAMED #10 & TOP MDR PROVIDER

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022

If you're experiencing a security incident or breach contact us 1-866-579-2200 or +44 (0)8000 443242

eSentire, Inc. is the Authority in Managed Detection and Response, protecting the critical data and applications of 1500+ organizations in 80+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts, Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.