Put the 'R' Back in MDR.

Towing the Line Between Machine and Human Response Actions

digital hands®

Table of Contents

Combating the Modern Threat Landscape with MDR

The typical security operations center (SOC) faces an unenviable, if not untenable, scenario. The security perimeter is nowhere in sight, the threats are multiplying daily, and the alerts are barraging analysts from everywhere. The sheer rate of attacks on an organization — 1,636 per week on average — has doubled in the past three years.[1] Worse yet, new emerging threats may require new skills and new tools to combat, putting even more pressure on security teams that are already stretched thin.

Many organizations are recognizing that their in-house SOC cannot keep up with the growing number and impact of cyber threats. In response, the market has evolved to offer managed detection and response (MDR) services — turnkey solutions that deliver improved threat detection monitoring and response, along with unified visibility and greater expertise. These solutions provide the speed and velocity necessary for keeping up with attackers.

When implementing a security program, CISOs typically want assurance that they are:

- ✓ Detecting real threats and minimizing false positives
- ✓ Spending time and resources in the right areas
- ✓ Detecting and actioning on threats faster (reducing their mean time to detect (MTTD) and mean time to respond (MTTR))
- ✓ Constantly improving and maturing their security posture

MDR delivers on these objectives through the right blend of experienced security professionals, artificial intelligence (AI) and automations, and technology — while fusing it all together into a unified view to help security teams detect and respond to threats more effectively. But many emerging MDR solutions fall short because they rely entirely on automations, claiming to eliminate the need for human response.

This ebook discusses why and how fast response must balance automation with human expertise — and what to look for in an MDR solution that delivers the assurances CISOs want.

[1] Check Point, July 2024

What is MDR?

Managed Detection and Response (MDR) provides 24/7 remote security operations, combining advanced technology with human expertise to detect, investigate, and mitigate threats in real time. MDR proactively monitors your environment for indicators of compromise, enabling swift detection and response to threats before they can disrupt your business. By integrating with your existing security tools and providing tailored response actions, MDR ensures comprehensive protection while aligning with your organization's specific needs.

The Name of the Game: Getting There First

Speed is crucial when you're trying to outmaneuver today's stealthy intruders, who can move laterally through the network in as little as two hours after initial entry.[2] Yet it takes the average organization at least two days to detect a network compromise.[3] Some data even puts the mean time to identify a breach at an average of 194 days.[4] That's a big reason why in cybersecurity, "the house" doesn't always win.

Ransomware is just one of many motivators for the SOC to catch up with this age of speed. In only 12 months, ransomware attackers have evolved to deploy payloads nearly 10X faster: within five hours of initial access instead of four and a half days.[5] For defenders, every second counts when it comes to response. **And that's where MDR comes in.**

[2] CrowdStrike, April 2023
[3] Anomali, 2022
[4] IBM Security, 2024
[5] Secureworks, October 2023

MDR helps solve four core SOC challenges

1 / 4

The need for speed

You can't afford to lose valuable time piecing together data from disparate tools and logs and sifting through alerts. An MDR partner is an extension of your internal team, quickly responding to threats and mitigating them on your behalf.

2 / 4

Proactive security

Attackers are changing their tactics all the time, yet many tools can only identify known threats. By monitoring for threats 24/7 and responding to them in real time, your MDR team can make proactive decisions that stop threats before they enter your environment and contain them before they inflict real damage. This team will also create playbooks to increase response times and combat threats more effectively.

3 / 4

Lack of visibility

The disparate security technologies in the SOC create silos that lead to issues like low-fidelity alerts, alert fatigue, and visibility gaps. MDR brings all the core technologies into one place, enabling the SOC team to view events from separate platforms, and then correlate and enrich them through automations. The outcome is that the analysts receive not simply an alert but a complete story that enables them to take precise and quick action.

4 / 4

Security talent shortage

The cybersecurity talent gap is estimated at 225,000 in the US alone[6], leaving many security teams stretched thin and unable to cope with the massive volume of attacks. An MDR solution is a force multiplier, allowing organizations to better use the security resources on hand and lowering recruiting, training, and retention costs.

To solve these challenges effectively, your MDR partner needs to balance automation with expert-driven, adaptable responses. **People excel where machines don't and vice versa — but together, they deliver an optimized approach that responds to threats with precision and speed.**

[6] Lightcast, Q2 2024

Machine vs. Human Response Actions: Which Should You Trust?

Two of the biggest trends in cybersecurity today are automation and AI. Automated actions that handle routine steps like correlating data from multiple sources can save analysts a tremendous amount of time. Not surprisingly, practitioners rank cybersecurity automation as the emerging technology that will have the most positive impact on their ability to secure their organization.[7]

But automation and AI are not a cure-all. A machine can only effectively automate workflows that block known threats while AI is essentially learning from human actions. Let's take a deeper look.

Machines

AI excels at quickly analyzing vast amounts of data, correlating data from multiple sources, and summarizing it. This process can help analysts find the proverbial needle in the haystack faster without having to swivel between consoles. But AI has various risks and limitations. **AI models:**

- Can make mistakes such as false positives *(leading to unnecessary alerts)* or false negatives *(providing a false sense of security)*
- Lack transparency, which means analysts don't have visibility into how AI arrives at specific conclusions
- Can easily overlook anomalies that don't fit a predefined pattern and don't have the ability to understand nuances

When an analyst consistently responds to a threat in the same way, the AI could create a rule that does the same thing automatically. This process is like creating a playbook. The AI engine adds a little efficiency and intelligence, but the automation is still based on human inputs.

So, if your humans have bad inputs *(for example, by taking the wrong actions)*, your AI automations will repeatedly fail in detecting and responding to threats. Not all automations are AI driven, but all require playbooks — in other words, humans to create and maintain them.

[7] ISC2, 2023

Humans

While automations can deliver expected outcomes faster and eliminate some of the manual work, they cannot replace humans entirely. **You need people for response actions such as:**

24/7 cyberthreat monitoring and response

For known threats, you can automate response actions such as blocking malicious IP addresses, isolating hosts, or resetting a user password. But for unknown and emerging threats, you need skilled analysts who can react to a potential threat based on threat intelligence as well as their knowledge and experience. Additionally, humans need to customize the threat detection and response rules to your needs, such as time-based custom triggers, to minimize disruption.

Threat containment

The faster you contain a threat, the less damage it will cause to your environment. You need humans to tailor the response actions — such as blocking and unblocking users, email senders, and application access; and isolating, wiping, or rolling back endpoints — to your operational needs and policies. For example, let's say you detected malware on a device. Isolating the system from the network can prevent lateral movement and stop the spread of the infection to other devices. Since some malware is designed to steal data like user credentials and web session cookies, containment could also include blocking the user's access from all critical systems and applications until you further investigate the scope of the threat and mitigate it.

Incident response

The objectives of incident response include neutralizing active threats and preventing threats from spreading further or reoccurring. Traditionally, MDR solutions did not include incident response. But customers now expect their MDR vendor to play a role here, which can be as small as working directly with forensic investigators to provide the right data. Or it could entail developing an incident response plan with prescribed response actions that are customized to the customer's environment and serve objectives such as neutralizing a specific threat.

Root cause analysis

Identifying the root cause of an incident, whether it's a software vulnerability or a gap in security policies, is a proactive way to address vulnerabilities and prevent a future incident. Your MDR team should customize the root cause analyses to fit your infrastructure and specific configurations so you can implement targeted remediation.

Regular health checks

To help you continuously improve security, some vendors go beyond threat detection and response to offer routine evaluation of your security posture and response readiness. These response actions go a step farther to help you continuously improve your security posture and prioritize risks based on your business needs. This is another area where human expertise is indispensable and can provide guidance on how you can mature your security approach and improve the effectiveness of your stack, procedures, and operations.

To Automate or Not to Automate?

A complete defensive strategy includes both reactive and proactive actions. Which of these you automate depends on whether the threat is known or meets certain predefined rules. For anything else, you most likely need an analyst's intervention. **Here's how this may look:**

Scenario 1

You have created a set of rules, such as detecting a call to a command-and-control center by a device, to respond reactively to a malware infection. When your technology detects the behavior that meets the predefined rule, an automated response could be triggered by default. This automation responds to a high-risk activity where there's no uncertainty about the threat.

↗

Scenario 2

Based on your threat intelligence feed, your SOC learns about a threat that's spreading rapidly in the wild. Your analysts proactively query your environment, searching for indicators of compromise (IoCs) If they detect these IoCs, they isolate the affected endpoints to prevent lateral movement and conduct further analysis to determine the scope and impact of the threat.

↗

Scenario 3

Your MDR provider detects a confirmed threat in one customer's environment or receives intelligence from a security leader about active targeting in a specific sector. Human threat hunters leverage both manual expertise and automated tools to proactively search for similar indicators of compromise (IoCs) across other customer environments. By identifying patterns and trends early, they mitigate potential threats before they can impact additional customers.

↗

Effective security is not about how many response actions a solution can automate. What differentiates an expert MDR partner from a mediocre one is their understanding of your environment (e.g., critical infrastructure, line-of-business applications, business needs) and ability to improve your security posture with a flexible approach.

You may want certain response actions fully automated or you may want your provider's human team to investigate. You may have a small in-house team who needs to augment their capabilities. Or you may be a more mature organization that wants faster outcomes and needs help leading with innovation and automation, defining playbooks, and refining the AI models that will execute in your environment. **A flexible and experienced MDR provider will meet you where you are — and customize the solution accordingly.**

What to Look for in an MDR Solution

A CISO's definition of success may vary, but there are some common expectations, such as having a holistic understanding of their environment, detecting real threats and actioning on them faster, ensuring resources are spent effectively, and maturing their security posture. To achieve these outcomes, an MDR solution needs the right blend of people, advanced technology including automation, and mature processes. The following capabilities can help you evaluate the effectiveness of an MDR vendor in executing your objectives.

1. Flexible Model That Serves as a Force Multiplier

A flexible, bespoke partner who understands the uniqueness of your organization will tailor your MDR solution based on your risk tolerance and objectives. The provider will take the time to understand your requirements and develop playbooks that integrate seamlessly into your process. For example, the vendor can customize threat detection and response rules to your needs, such as time-based custom triggers, to minimize disruption.

> Let's say your typical IT admin works regular office hours. If the admin account starts making a slew of changes to the system after 6 p.m., it could be a sign of malicious activity like a ransomware attack. You could set an automated rule that would proactively disable the admin account until an analyst can investigate further.

To offer these kinds of customizations, your partner needs a deep understanding of your environment. Automations or playbooks are simply not effective if they aren't pertinent to your organization.

2. Mature, Proactive Capabilities with a Robust Content Library

The more visibility your provider has, the more effective the response actions will be. But you don't necessarily need the MDR vendor to manage your entire stack. A mature solution will offer an alternative such as API connectors, even if these connectors only push the data one way. In a critical situation, you don't want a provider who will simply say they couldn't block a threat because they couldn't access something.

Another indicator of maturity is how forward-thinking the MDR provider is. You want to partner with someone who's not always waiting for alerts but proactively does research, keeps an eye on what's happening in the wild, and looks at threat feeds across different sectors. A skilled threat hunting team will develop new hunt packages based on all that information and run them against your environment retroactively.

> Think of these proactive activities as a law enforcement officer patrolling a neighborhood rather than waiting for a call from dispatch about a potential crime in progress. A patrol officer who's familiar with that beat will immediately know when something looks suspicious and investigate proactively. The same is true for threat hunters, who can look for IOCs and run detections retroactively to understand the scope of threat.

3. Fast Containment Actions to Minimize Impact

When you engage an MDR vendor, you should constantly see improvement in performance, based on metrics like mean time to detect, mean time to respond, and mean time to contain.

> The bottom line is for you to be better off today than you were yesterday, which means the MDR solution needs to provide a unified view of your environment and action on threats as quickly as possible.

Look for a vendor who effectively combines skilled experts, custom-tailored playbooks, and automated actions to prevent the spread of attacks and minimize their potential damage.

4. Expertise to Consistently Improve Your Security Posture and Maturity

A proactive partner who's invested in your success can help you mature your security program rather than only being concerned with defending your environment. **Look for a solution that:**

- Provides strategic guidance, along with tactical execution, that improves your security posture continuously.
- Harnesses the "crowdsource effect" that allows the entire customer base to benefit from threat intelligence.
- Offers transparency and insights into the threats, responses, and trends observed across your organization through regular security posture reports and a unified customer portal that serves multiple personas.

Final Thoughts

As AI technology continues to mature, automated workflows will further improve the efficiency and effectiveness of security operations. But don't let fully automated solutions fool you. Machines may be faster, but they're far from being more intelligent — or precise — than humans.

Automate actions that are low risk, clear cut, or routine.

But when the stakes are high, the situation is ambiguous, or the behaviors are nuanced, ensure you have a trusted, highly skilled team of humans who can follow through, provide guidance, and give you the confidence that the next step to take is the best one.

Why Choose Digital Hands

Digital Hands is a firm believer in putting the “R” back into MDR by combining extreme, smart automations and flexible solutions with a SOC team who has deep knowledge across a broad array of technologies and industries. Our customizable, customer-centric response actions go beyond generic playbooks to fit your unique environment and business objectives.

Many vendors boast hundreds or thousands of automated actions. Yet they stop short of explaining which ones are meaningful for your use cases. Digital Hands is not simply a vendor. We are a partner who focuses on delivering you an outcome of being truly secure rather than merely boasting stats.

With Digital Hands, you get response actions that:

- ✓ **Take minutes or even seconds** rather than hours or days
- ✓ Could be **fully automated or require human intervention** — your choice
- ✓ Are based on **custom rules designed to fit your requirements** while minimizing disruptions
- ✓ **Proactively block threats** before they can inflict damage
- ✓ **Combine machine speed with human intelligence** to stay ahead of bad actors

About Digital Hands

Digital Hands is a firm believer in putting the “R” back into MDR by combining extreme, smart automations and flexible solutions with a SOC team who has deep knowledge across a broad array of technologies and industries. Our customizable, customer-centric response actions go beyond generic playbooks to fit your unique environment and business objectives. Many vendors boast hundreds or thousands of automated actions. Yet they stop short of explaining which ones are meaningful for your use cases. Digital Hands is not simply a vendor. We are a partner who focuses on delivering you an outcome of being truly secure rather than merely boasting stats.