Beyond SIEM and SOAR:

The Overlooked, Critical Component of Managed Detection and Response (MDR)

digital hands

Table of Contents

The Need for Speed

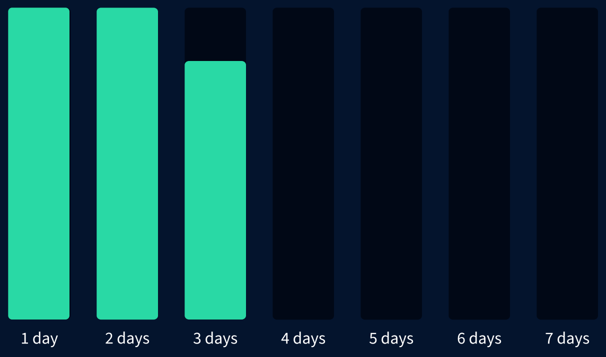
Speed is everything in today's cybersecurity landscape. The adversaries are growing faster and stealthier, while cloud-first environments and hybrid workplaces make breaches harder — and slower — to detect. It only takes an hour or less for an attacker to move laterally within your network after the initial compromise.[1] But if you're like the average organization, detecting the unwelcome intruders may take you at least 10 times longer — research shows that the mean time to detect a network compromise is 2.8 days.[2]

As cyber threats continue to evolve at breakneck speed, organizations are recognizing that their in-house security operations center (SOC) can't keep up. An estimated half have turned to outside support for their security.[3] But, while these outsourced services address pain points such as lack of in-house talent and expertise, there's a notable shift in what organizations expect from their security partners. Traditionally, managed security services providers (MSSPs) focused on identifying suspicious behaviors — usually based on rules — then throwing the alerts back over the fence to their customers. This approach was helpful for alleviating issues such as alert fatigue. But today, when seconds count, you need more.

Proactive, advanced security is essential when threats move at an unrelenting pace. This includes monitoring your environment around the clock, detecting threats in real time, and responding quickly. That's why organizations are moving toward advanced managed security services, with 79% planning to upgrade from legacy MSSPs to managed detection and response (MDR).[4] The MDR solution marketplace, however, can be misleading. Many vendors tout their technology's bells and whistles while trivializing the glue that holds security programs together — people.

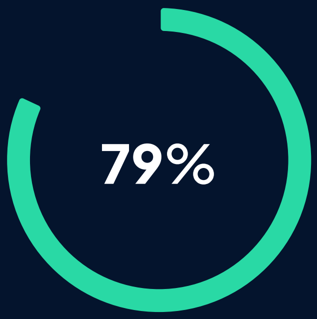
This e-book takes a look at the critical layers of an MDR solution, including the human layer, and how you can implement MDR for long-term success.

It only takes an hour or less for an attacker to move laterally within your network after the initial compromise.[1]



But if you're like the average organization, detecting the unwelcome intruders may take you at least 10 times longer — research shows that the mean time to detect a network compromise is 2.8 days.[2]

An estimated half have turned to outside support for their security.[3]



That's why organizations are moving toward advanced managed security services, with 79% planning to upgrade from legacy MSSPs to managed detection and response (MDR).[4]

[1] CrowdStrike, Lateral Movement, April 2023
[2] Anomali Cybersecurity Insights Report, 2022
[3] Dell Technologies/VansonBourne, Global Data Protection Index, 2024 Special Edition
[4] LogicHub/Osterman Research, New Research Report Highlights Significant Shift to Managed Detection and Response (MDR) Services, June 2022
[5] KMPG Cybersecurity Survey, May 2024

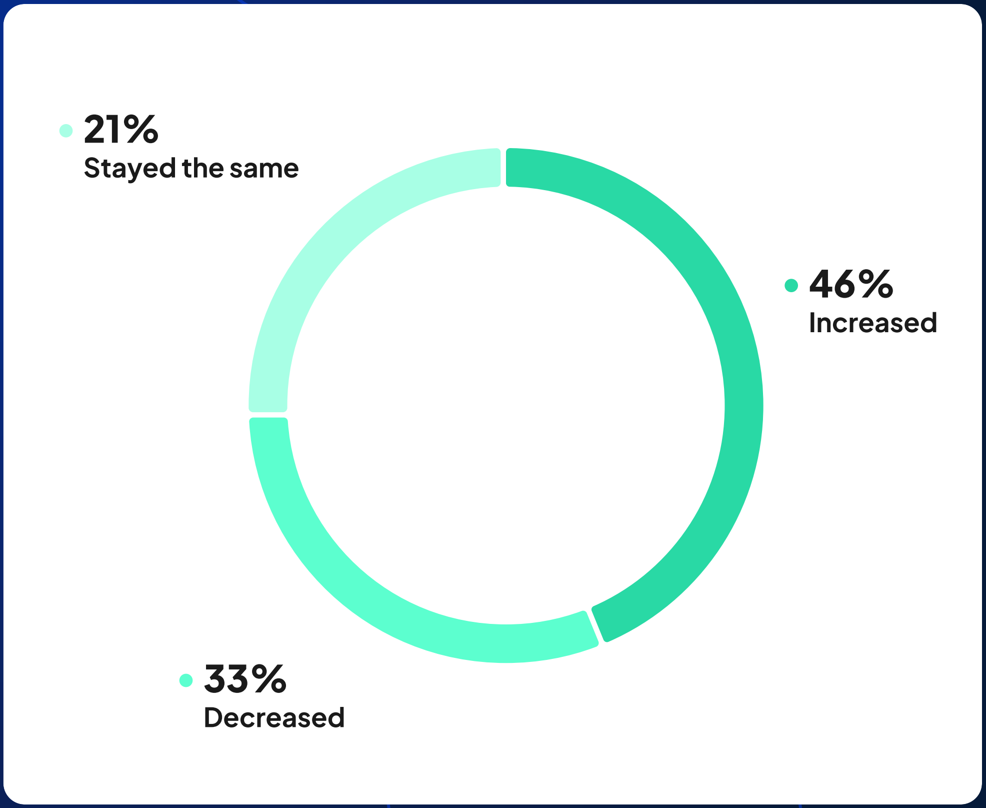
Beyond the Automated Platform

If the burgeoning MDR market is any indication, more organizations today want a partner who can go beyond simply identifying threats. The majority of MSSPs are already offering some type of MDR services, and estimates show the market growing at a 25.8% compound annual growth rate[6].

When navigating this market, many CISOs focus on the vendor's platform (typically a SIEM and SOAR) and its technical capabilities. A common question they may ask is how many automations the platform has. It's a valid question, of course. Automation is essential because, in theory, it should accelerate the speed of response. But automation, in and of itself, doesn't equal action. For that, you need people. Many vendors selling automated platforms position themselves as an MDR solution. The question you should ask yourself is this: **Are you looking for outcomes such as reducing your risk holistically, decreasing your team's workload, and gaining 24/7 access to experts who can help you stay secure?**

If the answer is yes, then simply buying a platform to manage in-house isn't going to fix your issues like alert fatigue caused by excessive false-positives or detections with no context. What you're more likely to get from a standalone platform is the added burden of managing this complex system and then relying on a portal to figure out what alerts need your response.

Almost half of surveyed SOC practitioners say their average time to detect and respond to incidents has increased in the past two years.[7]



[6] Sophos, MSP Perspectives, 2024
[7] Morning Consult/IBM, Global Security Operations Center Study Results, March 2023

Why People Are Important in This Age of Automation

Only 34% of surveyed MSSPs that provide MDR services have an in-house SOC.[8] This is a problem. These providers may have the best technologies and the most robust security policies in the world, but without people to run and execute them, they can't offer you fast response action.

Sure, if a vendor touts thousands of detections and shows you dozens of pages worth of automations, it sounds impressive. **However, automated responses are built based on known threats and adversary tactics.** If you've detected and responded effectively to certain threats in the past, then automating those response actions is a good call. That said, the threat environment changes every single day, so you're not guaranteed the same positive result 100% of the time.

Artificial intelligence (AI) that powers the platform can also learn and make adjustments, but it's never going to be as good as experienced humans who are digesting the data and making informed decisions.

AI systems also excel at identifying behavioral anomalies. But if an exploit uses regular vectors and there are no known bad signatures, how certain are you that your "advanced AI" will spot the deviation from the norm? No technology provider can guarantee 100% that the AI will succeed every time — and that creates a struggle because your internal team has to pick up the pieces.

So, even with automated responses, people remain the central resource for security operations.

[8] Sophos

The technology is only the facilitator, and you need human experts at different stages of your threat detection and response, including:

- ✓ **Onboarding** — to select and optimize the right security data sources logs and create correlations.
- ✓ **Tuning and optimization** — to create rules based on your environment and review the data to ensure noise is eliminated.
- ✓ **Customization** — to focus your threat detection and response activities on what's important to you and on your use cases.
- ✓ **Validation** — to ensure your rules (such as those aligned with specific MITRE ATT&CK tactics) are supported with quality content.
- ✓ **Threat detection and response** — to provide 24/7 "eyes on glass" coverage and ensure real-time response.
- ✓ **Proactive response** — to proactively block known threats before they can enter your network, leveraging institutional knowledge and threat intelligence gained in other environments across the entire customer base.
- ✓ **Compliance** — to help you decide strategically which logs need to be stored so your data doesn't waste storage capacity.

Without human expertise, you won't get the expected outcomes from your provider's technology platforms like SIEM and SOAR. In fact, people make up half of the critical MDR layers, as we explain further.

Humans vs. Machines: When Do You Need Human Intervention?

The mindset that cybersecurity is “one size fits all” is outdated. Every organization is different. This is where composable security comes into play because it’s tailored to your individual use case.

To get the greatest value and effectiveness from your security, you need humans to analyze the inputs and properly tune, configure, and manage the systems. **For instance, not all ingested logs have security value for your organization — what’s valuable in one environment might not be in another.**

Humans can also tailor your security to your technology environments *(e.g., cloud, network, server, mobile devices)*, your business model *(e.g., hybrid or remote workplaces, international vs. national footprint)*, and other needs *(e.g., compliance and regulatory requirements).* **The difficulty of cybersecurity is that’s it’s both broad and deep. You need to know a lot of things about a lot of things, and this breadth of required knowledge is perpetually growing.**

> Think of the **Log4j** vulnerability. When it first surfaced, no security technology understood it and it left many systems and applications exposed. It took many security professionals to respond quickly by manually creating rules and processes before the vendors finally caught up. And even then, some security vendors rushed the process and their fix was ineffective, so it still required human intervention in the SOC to fix the issue.

Zero-days and creative hacks aren’t going anywhere — which means you’ll always need people who can synthesize the issue, verify the proposed vendor fixes, and then applying their knowledge of your unique environment to the ultimate execution.

Four Critical MDR Layers Beyond the SIEM and SOAR

1 / 4

Human intelligence

From confirming that meaningful data sources with security value are ingested and that ingested data is accurate, to ensuring the data is parsed correctly and the fields are populating as expected, you need humans. Human intelligence comes at the forefront to build confidence in your data and detections — and ensure you're getting expected outcomes from your machine intelligence.

2 / 4

Machine intelligence

Whether it's automating initial response actions (e.g., isolating the endpoint, resetting passwords, disabling user access), correlating and enriching data, or providing cross-threat and cross-industry context, machine intelligence enhances threat detection and response to improve speed and accuracy.

3 / 4

Human response

As noted previously, you need humans for actioning response based on factors like context, industry-specific threats, and your distinct network architecture and user base. An MDR provider who has the right mix of people and technology can offer you the flexibility to automate responses based on your objectives — while freeing up skilled human experts to navigate situations that require human intervention.

4 / 4

Visibility and presentation layer

You need a portal that allows you to collaborate and communicate with your MDR experts, as well as take action based on how hands-on you decide to be. For instance, if you want to approve certain response actions, you can do so immediately through the portal without the need to speak to your outside security team.

4 Steps to Implementing an MDR Solution

One of the biggest advantages of working with a smart MDR provider is flexibility. You can design the solution in a way that maximizes your existing security investments while gaining the right-size expertise when and where you need it. Here are the core steps to implementation.

1. Discuss your goals and desired outcomes

Your MDR provider brings a lot more to the table than technology. This team of experts has deep knowledge of best practices not only across a wide range of technologies but also across industries, environments, and use cases.

> Your deployment process starts with a consultative conversation around topics such as your risks and security posture goals so you can implement your managed detection and response strategically. The MDR provider can meet you at whatever maturity level you are currently and devise a plan that helps you continuously improve your cyber resiliency.
>
> Becoming more resilient is the best way to stay ahead of the adversary. A proactive partner can help you implement a smart and intuitive system that allows you to take control of your security while making simple response decisions with the click of a button.

2. Choose your tech stack

If you work with a partner who offers a composable security model, you'll get the most from the investments you've already made — without having to "rip and replace" or buy a new solution. A composable model supports a broad array of technologies and can correlate and enrich events across all of them.

> Bring your own stack — or don't. A vendor-agnostic MDR provider will work with whatever technologies you have in place or want to deploy. If you don't have an in-house SIEM, they can integrate their own into your environment to capture the necessary telemetry. Or you can use a mix of your stack and theirs.

Once you've selected your security stack, your partner will add a security fabric (typically proprietary) and capabilities on top. This security fabric also weaves in threat intelligence and automation so your external security team can contextualize threats and respond quickly.

3. Test and validate your deployed technologies

After your SIEM and SOAR are deployed, you need to tune the platforms and confirm that your content is performing as expected. Some of the questions the deployment team will ask include:

- Do we have the right data?
- Is the data being parsed correctly?
- Are threats or anomalous behavior being detected?

Your MDR partner will use a range of techniques, such as breach and attack simulation, to validate performance. This process may entail several iterations and tunings to ensure the detections are working.

4. Customize and operationalize your MDR service

An MDR partner who's willing to flex with you will offer numerous customizations based on how you want to run your security operations and on your level of comfort with your external response team. During this phase, expect to meet with your MDR team to discuss a variety of operational aspects.

Examples of what you should be able to customize include:

- What response actions you want to fully automate
- What escalation procedures analysts should follow
- What detection use cases are applicable to your environment
- What custom parsing and tagging your data needs *(e.g., nonstandard data sources or specific fields or tags from event data)*
- What specific automated reports you want to receive or what data you want to see presented in your dashboards

The typical implementation timeline is around 30 days; however, this is contingent on your situation and internal resources.

What to Look for in a Successful Partnership

When you're considering an MDR solution, think of the vendor's technology as table stakes. Every vendor offers some type of platform, but what matters is how it's implemented, optimized, and used. This is why it's important to evaluate the human factor and the provider's security operations.

These are the four main criteria to consider:

Expertise

Think of your MDR provider as your trusted consultant. What do you want them to bring to the table? Tenure and continuous training are just a start. They need to the same institutional knowledge that you have, as well as to understand your business, requirements, and limitations. They also need the ability to continuously mature your operations through the crowdsourced effect of referencing thousands of other customer environments. Additionally, a partner who cross-trains these experts can offer you better continuity — cross-training helps retain institutional knowledge during staffing turnovers.

Flexibility

In addition to a composable and vendor-agnostic model, look for flexibility in the budget. But keep in mind that a smart partner who has your best interest in mind may dissuade you from a specific technology that's too expensive to operate and doesn't get you a good return on investment.

Transparency

Gone are the days when you trusted the wizard behind the cloak to keep you secure. You need real-time visibility into your security posture — mean time to detect, mean time to respond, mean time to contain, investigations completed, automated actions, and so forth — so you're informed at all times about what's happening inside your environment and why. There's also growing pressure from the board of directors and regulatory bodies to confidently show proof that you're secure. The best way to provide this transparency is through a tool such as a user-friendly portal.

Outcomes

What you're buying from your MDR provider is confidence that you're secure without adding unnecessary overhead. You want peace of mind that your external team will respond quickly and effectively without putting any extra burden on your internal resources. And ultimately, long-term success is about taking your security to the next level — you should be seeing consistent improvements in your security posture.

Going Beyond SIEM and SOAR with Digital Hands

The Digital Hands mission — to “get there first” — guides our expert team to deliver smart and flexible security solutions. Powered by our proprietary platform and other best-of-breed technologies, our 24/7, U.S.-based SOC augments your internal resources with experts who have more than 20 years of experience in staying ahead of threats.

We don’t believe in a “rip and replace” approach, black boxes, or rigid solutions.

Nor do we throw alerts back to you that overload your team further. Instead, your Digital Hands team:

- ✓ **Offers a composable security model that enables you to bring your own technology** — as well as leverage ours — for faster and more accurate action.
- ✓ **Provides complete visibility into your security operations through our CyGuard® Portal** — so all your tactical, operational, and strategic data is unified in one location.
- ✓ **Supplies alerts enriched by human expertise** so you can make an informed decision quickly.
- ✓ **Ensures your issues are resolved quickly** and definitively while proactively managing and improving your security posture.
- ✓ **Delivers extensive automation capabilities and threat intelligence though CyGuard Maestro™**, our collection of proprietary technologies built on cloud-based architecture.
- ✓ **Arms you with actionable insights** to ensure your executives can invest in security strategically.

Ready to stair-step into the next evolution of threat detection and response?

The MDR marketplace is awash with vendors promoting technology capabilities that do little to streamline your workflows, keep you compliant, and reduce your workload.

Contact Digital Hands to learn how our Real-World MDR solution combines human expertise, advanced technology, and automated responses at machine speed to deliver unparalleled protection against real-world threats.

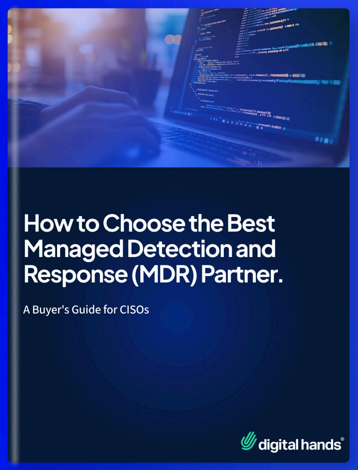
✉ Contact us at www.digitalhands.com/contact

Guide

Not sure where to start?

Download our Buyers' Guide for CISOs to discover the top criteria for evaluating MDR services and achieving the outcomes your organization needs.

Download



How to Choose the Best Managed Detection and Response (MDR) Partner.

A Buyer's Guide for CISOs

digital hands