LogicHub

White Paper

The Definitive MDR Buyer's Guide:

Everything You Need to Know to Choose the Right Managed Detection and Response Service

LogicHub

Table of Contents

What Is MDR and Why Is It Important?

For the last 20 years, organizations have been reliant on Security Information and Event Management (SIEM) systems, but this is no longer enough. Deeper detection and smarter responses to highly sophisticated threats are now a necessary part of a security stack.

As a result, new security tools have emerged that focus on an intelligent and managed response to threats. Managed Detection and Response (MDR) is at the forefront of this security transformation, along with XDR (eXtended Detection and Response), EDR (Endpoint Detection and Response), which is sometimes called EDTR (Endpoint Detection and Threat Response).

The evolving threat landscape requires new security tools and processes that focus on an intelligent and managed response to threats. Managed Detection and Response (MDR) is at the forefront of this security transformation.

Organizations are finding that they require deeper detection and smarter responses to highly sophisticated threats to protect across multiple, complex environments. It's safe to say that just about every organization has a stack of tools generating too many alarms and not enough time in the day to effectively analyze and respond to threats fast enough.

As a result, organizations are turning to a managed detection and response (MDR) service to augment their security operations to achieve 24x7 threat detection and incident response services without overhead necessary to do it on their own.

If you are considering implementing MDR, or if you already have one and think it should be doing more for you, this guide offers critical considerations to identify an exceptional MDR for your organization — as well as what sets LogicHub apart.

Critical Challenges Facing Organizations

Every organization faces similar security challenges. The problem can be summed up in one simple statement: ***Too much data and too few people.***

- Most security teams don't have access to the skills or personnel necessary to effectively manage the 20+ tools they have in their security stack.
- The proverbial "single pane of glass" still very hard and expensive to build, particularly on your own.
- There are too many alerts to investigate, and in many cases 95% or more are false positives.
- Security teams are bogged down by repetitive and overly manual investigation and triage processes that take too much time to perform in depth, leaving them vulnerable to attacks that get overlooked.
- Security teams struggle with detecting the many threats that hide in the gray area between obviously bad and obviously good activity
- Most security analysts spend a significant amount of time on mundane tasks that don't adequately utilize their training or skills.
- Automation platforms are either not powerful enough to execute critical playbooks, or they're too expensive to purchase and deploy, and fail to deliver a positive ROI.

AI and Automation Is the Future of Detection & Response

"LogicHub has based its platform on expertise automation, blending expert systems with deep neural net architecture. The engine learns and updates its own logic to make more accurate decisions like a human analyst."

— Gartner, 2021: Emerging Technologies: Tech Innovators in AI in Attack Detection

Why Businesses Are Choosing to Implement an MDR Service

> ***"By 2025, 50% of organizations will be using MDR services for threat monitoring, detection and response functions that offer threat containment and mitigation capabilities."***
>
> — Gartner Market Guide for Managed Detection and Response Services – October 2021

Successfully managing an effective detection and response program requires skilled staff, an extensive security tech stack, and the ability to provide 24x7 coverage. This is increasingly difficult to do as organizations face a persistent and growing shortage of skilled security analysts. High staff turnover has become a pervasive issue, creating additional gaps in processes and skills that leads to a continual loss of tribal knowledge. Many organizations find that the security team they do have is overwhelmed with alert triage and reactive cycles on low-value security tasks.

In the face of these challenges, many organizations have turned to managed detection and response (MDR), which allows companies to rely on expert services for threat hunting, detection, and incident response. Organizations are turning to the service to augment their security operations to gain 24x7 threat detection and incident response services without the prohibitive overhead.

1. Lack of Threat Visibility

Even within organizations that have the right security in place, there are blind spots. Not all security tools are being monitored. There may be clues that something is missing, but the evidence is hard to grasp. Most organizations are generating so much data that they are unable to effectively sift through and identify real threats throughout the environment.

2. Limited Time and Resources

Both small and large organizations experience an explosive volume of alerts, which can be overwhelming to say the least. That fact is that it is simply impossible to keep up with the sheer volume of security alerts. And maintaining security without increasing staff is a huge IT challenge, regardless of the size of the team.

3. 24/7 SOC challenges

Not every organization can or wants to build an expensive, complex 24/7 SOC. It is difficult to monitor an enterprise 24/7, but attackers don't work on banker's hours. If you don't have round the clock coverage, you have a higher risk exposure. The reality is that every organization — whether a small business or massive empire — needs 24/7 security protection.

4. Growing Resources Gap

Staffing a 24x7 SOC requires far too much overhead for most mid-sized organizations. Even with the available staffing budget, finding and retaining skilled security staff is becoming an impossible task and staff turnover is far too common. Constant churn leads to broken detection and response processes and a continual loss of tribal knowledge.

5. Alert Fatigue Impacts Everyone

Alert fatigue is a widespread common phenomenon among IT security operations professionals. Multiple systems overloaded with data produce too many alerts for any security team to reasonably investigate in any given day. Alert triage is often done inaccurately, resulting in teams chasing down an overwhelming number of false positives while real threats go undetected.

> ***"The perfect storm of too many security tools creating too many alerts for overstretched security teams has created an urgent need for many organizations to move to more advanced managed security services."***
>
> — Osterman Research, 2022

Not All MDRs Are Created Equal

A three-person security team with 24/7 security responsibilities gets real value when its efforts are augmented by a managed detection and response (MDR) service. Corrective action after a security event can take place within minutes.

An effective MDR service should be able to answer "yes" to each of these questions:

1. Are operations fully transparent and customizable?
2. Is the entire security stack supported?
3. Are custom integrations supported?

Even some MDR providers themselves can suffer from the same issues as security teams. Why? Because MDR vendors often use the same kind of technology (generating noisy alerts) and solutions that demand more manual work instead of less. They try to fix this by just throwing more people at the problem, passing the cost on to the customer. This strategy simply renders many MDR services ineffective, expensive, or both.

Many MDR vendors often fail to support the entire security stack — requiring clients to only use their preferred tools and data sources. Even smaller teams of three or five people may use 30 or more different tools and sources in their stack, up to 40% of which aren't even supported by their MDR service. That's a huge blind spot.

At a Glance

Conventional MDR

- ⊘ Have cookie cutter content with standard rules
- ⊘ Have hidden or opaque detection content
- ⊘ Do not allow for customized detection content
- ⊘ Generate too much noise, including too many false positives
- ⊘ Require customers to wade through too many alerts
- ⊘ Lack rich case context
- ⊘ Do not provide actionable response suggestions

LogicHub MDR

- ✓ Over 600+ prebuilt detections
- ✓ MITRE ATT&CK® framework mapping
- ✓ Open and customizable detection content
- ✓ Continuously added new detections
- ✓ Rich, actionable cases instead of unmanageable and unimportant alerts
- ✓ Clear, actionable, one-click recommendations to respond to cases
- ✓ Automated triage of false positives
- ✓ AI-driven automation delivering unrivaled accuracy
- ✓ Full context on all cases

MDR Checklist: What to Expect from an Exceptional MDR Service

Given the today's threat landscape, 24/7 security coverage and quality customer support are necessities, not luxuries. Whether evaluating the quality of your current MDR service or looking to implement one, Gartner's industry research recommends that the right MDR service should include:

1. Integration with Your Entire Security Stack

A worthwhile MDR provider should already have hundreds of out-of-the-box integrations, but they also need to provide custom integrations quickly and at no extra cost. More importantly, they should be able to support your entire existing technology stack. There should be no need to rip and replace any of the significant investments a business has already made.

2. Mapping to MITRE ATT&CK® Framework

Existing protections (whatever they may be) should not only be supported, but also be mapped to the MITRE ATT&CK® framework. This enables teams to examine what the service detects as well as identify blind spots and gaps in detection. The MDR vendor should guide and advise customers on additional data sources and deployable detections to interpret and bridge these gaps.

3. Extensive Automation

Analysis, investigations, and swift, accurate, decision-making are all crucial parts of an effective MDR service. Many of these tasks can be fully or partly automated to augment a security team. The best MDRs automate whatever can be automated and leave time for security teams to focus on the most difficult challenges — so people can do what they do best.

4. Cases, Not Alerts

The right MDR service turns thousands of alerts into a handful of rich and actionable cases. Advanced automation, AI and machine learning triage alerts and consolidate the noise into a crystal-clear signal.

It should also be adaptable. To avoid repetitive alerts and even recurring cases, every escalated case from the MDR team should incorporate previous customer feedback. No customer should have to look at the same contextual piece of information again and again, because the system should be progressively learning.

5. Detection and Response Automation

Far too many services boast about detection but do little to help you practically respond. An MDR service should have automation tailored to customer needs to proactively take actions. Both feedback and customized detection response should match enterprise requirements so closely that each case alone is sufficient for a customer to make an informed decision. This process should allow customers to quickly view, understand and approve actions—ideally with one-click.

6. Complete Operational Transparency

Unfortunately, threat detection can be a world of smoke and mirrors. A vendor that claims "hidden" or "opaque" detections provides no detection application visibility for customers. To effectively shine a light on blind spots, security teams need this visibility to maintain their systems. Gartner emphasizes that visibility and transparency are paramount for a good MDR service.

7. Customizable and Adaptable to Your Business

It goes without saying that every organization is different, and customers should have the ability to customize all aspects of their detection and response processes. An exceptional MDR service uses an efficient yet customized, per-customer approach. When an MDR vendor escalates a case to a customer who requests a specific response be taken, the additional context should be incorporated into feedback for machine learning. Not all companies do this in the same way: one organization's desire for automation may be another's "business as usual."

8. Exceptional Communication

This one is so obvious; it seems odd to have to call it out. But poor communication with their current MDR provider is one of the top reasons security teams start shopping for another provider. Customers should expect full access to experienced security personnel who are dedicated to keeping their business secure.

LogicHub AI and Automation-Driven MDR

LogicHub's advanced AI technology and automation is the cornerstone of our MDR service. We integrate with your security stack to deliver 24x7 expert threat detection and automated incident response, based on the MITRE ATT&CK framework. Get complete visibility into all cloud, network, and user activity, close security blind spots, eliminate noise, and free your analysts to respond to real incidents.

Whatever your organization looks like, we deliver detection and response solutions that adapt to fit your requirements. As your business needs change, we grow with you — delivering deeper detection, faster response, and lower dwell times.

Whether you're choosing an MDR as an enhancement for or replacement of your current SIEM, implementing MDR for the first time, or looking to replace your existing MDR provider, here are eight ways the award-winning LogicHub MDR is different from the competition:

1. Support for Your Entire Security Stack & Integrations

LogicHub is vendor and data-source agnostic. Our technology can connect to any tool you have in your environment via automation. Even better? We're fully agent-less, which means we won't touch your production environment. We have hundreds of integrations available out of the box, and if you have a tool that we don't support, we will provide you that new integration in less than (3) weeks at no additional cost to you.

Gartner featured LogicHub as Tech Innovators in AI in Attack Detection in 2021, based on the award-winning automation platform that underpins our MDR service.

- *"LogicHub's attack detection innovation is 'decision automation.' It enables skilled hunters to encode their techniques, capturing their expertise."*
- *"AI-enabled solutions should move away from a 'black-box' approach towards explainable and customizable AI models that can be tuned based on analyst feedback."*
- *"The LogicHub platform blends expert systems with deep neural net architecture. If the individual makes a different decision from the engine, it learns and updates its own logic."*

2. Full Operational Transparency & Control

We offer complete transparency into how we operate. From detailed and KPI-driven dashboards to our detection playbooks, we'll show you exactly what we're doing and how we're doing it. This allows us to work with you more effectively to customize content that meets your specific needs.

We give you complete control over our automated incident response playbooks, allowing you to require one-click authorization before executing any action. That way you can queue up any action for immediate execution, while the only time and effort required of you is to say yes or no.

3. 24/7/365 Expert SOC Service

Our security experts collaborate with your team, monitor your entire security stack, and build custom content to generate cases — around the clock, 24 hours/day, 7 days/ week, 365 days/year.

4. Customized Support and Continuous Improvement

In addition to our 24x7 SOC-as-a-service, our SOC analysts continually work with you to create and update integrations, playbooks, and other product content to ensure you are always protected. Whether it's in response to new and evolving threats or to accommodate changes to your people, process, or technology, we'll deliver the solutions that you need — fully customized to your requirements.

5. Deep Threat Detections

LogicHub has more than 600 prebuilt detections using the MITRE ATT&CK® framework, with more added all the time. We provide tailored responses on a standardized system, which contrasts with other vendors' generic, opaque content.

Our detection playbooks rapidly perform accurate analysis, investigation, and triage, and automatically enrich every case with the context necessary to respond quickly and lower your mean time to respond (MTTR). That's why we can deliver an average MTTR of 30 minutes or less. And we map them directly to the MITRE ATT&CK framework to always ensure a best practices approach to detection and response.

6. Rich, Actionable Cases — Not Noisy Alerts

Our playbooks are designed to generate contextualized cases, not alerts. We consolidate alerts into cases and only escalate the most critical threats for customers to make decisions. Our service includes built-in case management in which we provide the case with full documentation of why we think it's a case. Then and only then do we send it over to you for review.

7. One-Click Automated Response

The LogicHub business model is built on full operational transparency for our clients, and you retain full control and visibility. We don't just monitor — we recommended actions with one-click responses delivered for your approval. Other vendors often do not provide remediation recommendations, leaving actions entirely up to customers.

8. Partnership with Our Customers

Our expert SOC team is an extension of your security team. LogicHub's outstanding team of security experts are some of the best in the business. They have decades of experience in threat hunting, detection, and response techniques, and have developed some of the most advanced playbooks in the industry.

Our clients enjoy full operational transparency and direct access to our customer success team who understand and advocate for your businesses' unique architecture and requirements. We are driven to deliver the best customer service in the industry and meeting the needs of the clients we serve.

LogicHub MDR

- Supports your **entire security stack**
- Captures and complements **tribal knowledge** (instead of replacing analysts and engineers)
- Features MITRE ATT&CK®-based **deep threat detection**
- Consolidates noisy and overwhelming alerts into **rich, actionable cases**
- Provides **automated one-click response** for easy decision-making
- Comes with a team of **24/7 security experts** dedicated to your protection

LogicHub

Awards

Gartner

- Demand-Side Innovator for AI in Attack Detection*

- Hot Company in Managed Detection & Response (MDR) Service
- Most Comprehensive Artificial Intelligence and Machine Learning

- Best Ai Threat Detection
- Best Security Orchestration, Automation & Response (SOAR)
- Best MDR
- Best Security Automation

SC AWARDS 2022

- Best Managed Detection and Response (MDR) Finalist

*(Gartner 2021 - Company Recognized in 2021 Gartner® Report titled, "Emerging Technologies: Tech Innovators in AI in Attack Detection — Demand Side")

About LogicHub

Founded by seasoned cybersecurity veterans from ArcSight and Sumo Logic, LogicHub is built on the principle that every process for threat detection and response can and should be codified and automated. LogicHub's managed detection and response (MDR) service is built on the LogicHub XDR/SOAR platform, which can be leveraged as a service or deployed as an independently managed platform.

LogicHub delivers intelligent automation-driven extended detection and response solutions that are flexible enough to fit any customer's requirements. LogicHub solutions adapt and grow with our customers as their needs change, delivering deeper detection, faster response, and lower dwell times.

© 2022 LogicHub® • 800 West El Camino Real, Suite 180 • Mountain View CA, 94040 • (650) 262-7690 • info@logichub.com