LogicHub

SOLUTION BRIEF

The Logic Hub MDR+ Difference

Automation-driven managed detection and response

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. And high staff turnover has become a pervasive issue, creating additional gaps in processes and skills, leading to the 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.

But not all MDR solutions are the same

As you embark on choosing an MDR vendor, it's important to be aware of some of the limitations from traditional MDR services:

1. Most primarily focus only threat detection, leaving you managing incident response processes
2. Many MDR vendors are limited to using a defined set of security tools, requiring you to buy or use specific vendor technologies for adequate visibility. This renders many of you preferred security acquisitions redundant, resulting in a partial or total loss of prior investment.
3. Some MDR vendors specialize in one or two types of detection, leaving you blind to attacks using different threat vectors. This leaves you on the hook to continue monitoring and investigating everything else.
4. MDR vendors frequently operate in a black box, providing limited access or details on what they're doing, how they're doing it, and when it's being done. This lack of transparency leaves you in the dark in too many situations and makes it difficult to truly understand what's being done to secure your network.
5. Many providers are overly dependent on manual threat investigation and incident response processes that can be skewed by individual analysts, leading to inconsistent detection, missing event context, and slower response times.

LogicHub MDR+ overview

LogicHub avoids the limitations of traditional MDR vendors, acting as a true force multiplier by augmenting your team with automation-driven threat analysis, detection and response, continuous threat hunting, and 24x7 expertise. And we provide full transparency into what we're doing and how we're doing it, at all times.

LogicHub MDR+ operates like a 24x7 SOC-as-a-Service, monitoring and analyzing all of your security event data, verifying and triaging threats, confirming threat detection, and automating incident response. Our MDR+ service also performs continuous configuration and optimization of custom playbooks, working with you to make sure that your environment is always protected.

And LogicHub MDR+ integrates with your existing security stack for complete visibility into your data, letting you continue using your preferred tools and protecting your security investment. We also give you the option to use to our cloud-based, fully managed SIEM, with no data restrictions, removing yet another source of operational overhead from your plate.

With LogicHub MDR+, you gain automation-driven detection and response services that provide:

- Accurate detection and response at machine speeds
- 24x7 analysis, investigation and triage of all security event and alert data
- Automated incident response playbooks with one-click execution
- Dedicated security analysts
- Continuously updated, expert content

Experience the LogicHub MDR+ Difference

Extensive integrations
We have hundreds of out of the box integrations. And our open API framework let's us add any new integration that you need in two weeks or less—at no charge.

Operational visibility
Our service is fully transparent. Full visibility into our detection and response playbooks and custom dashboards and KPIs show you exactly what we're doing and how.

Rapid customization
One size doesn't fit all. We'll work with you to quickly create custom detection and response playbooks adapted to fit your unique environment and needs.

Automation-driven processes
By leveraging the power of our SOAR+ platform, you'll get detection and response that's fast, consistent, and accurate.

Automated threat hunting
We'll build automated threat hunting playbooks that will augment and empower your staff to be proactive about advanced threat protection.

Cost effective protection
Our analysts work with your existing security stack to deliver expert detection and response so you can retain your security investment minimize operating overhead.

Get the most out of your MDR partnership

Choosing the right MDR partner and ensuring you have the most cost effective, proactive protection is critical to the success of your organization's security program. LogicHub's automation-driven MDR+ with 24x7 expert coverage empowers you to achieve true cyber resilience.

The MDR+ Difference

Capability	Traditional MDR	LogicHub MDR+
24x7 monitoring	✓	✓
False positive reduction	✓	✓
Expert investigations	✓	✓
Optional managed SIEM	Some	✓
Dedicated security analysts	Some	✓
Transparent operations	Some	✓
Adapts to your security tools	Some	✓
Autonomous threat detection	✗	✓
Automated incident response with one-click execution	✗	✓
Managed SOAR+ with individual customization	✗	✓
Continuously updated expert content	✗	✓

To learn more about the LogicHub MDR+ visit: www.logichub.com/mdr

LogicHub

a: 301 N Whisman Rd Mountain View, CA 94043
w: www.logichub.com
e: info@logichub.com
p: (650) 262-3756