LogicHub

ebook

8 REASONS

Automation is Critical for Effective MDR

Every security organization faces similar problems.

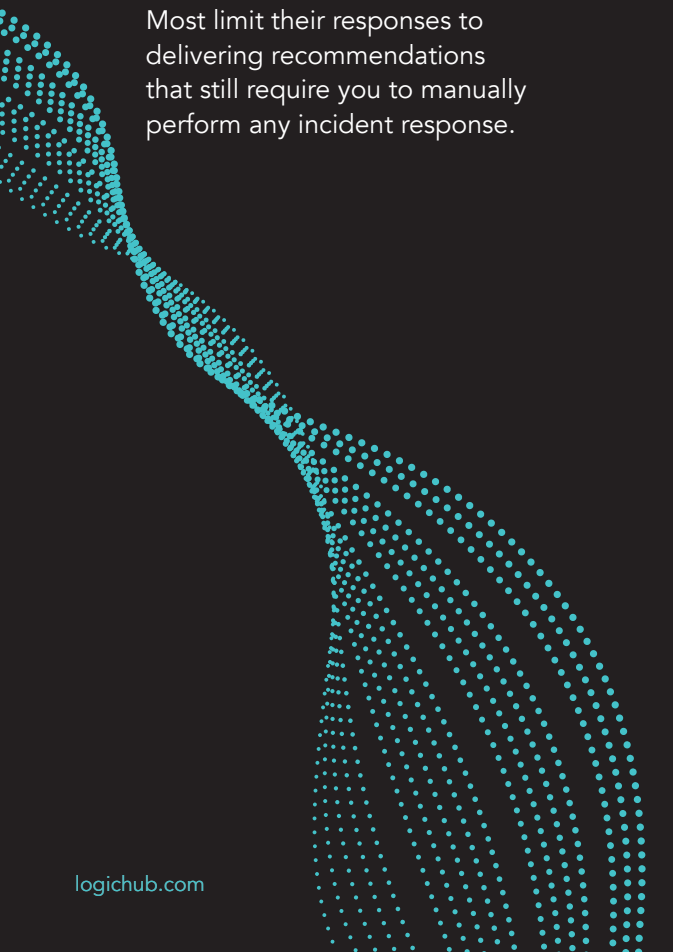
Detection and response is a critical component of securing your enterprise, but gaining deep visibility into the cloud, endpoints, networks and users, regardless of where your data resides, requires extensive resources that few organizations are capable of fully managing on their own.

Even with a highly trained staff and a broad array of security technology available, you probably have too many tools generating too many alarms, without enough time in the day to effectively analyze and respond to threats fast enough.

But you're still expected to deliver airtight security around the clock, no matter what it takes.

One of the biggest shortcomings of a traditional MDR provider, as well as almost every MSSP, is the lack of comprehensive response capabilities.

Most limit their responses to delivering recommendations that still require you to manually perform any incident response.



In response to these issues, many organizations are turning to managed detection and response (MDR), giving them access to 24x7 threat detection and incident response services without the overhead necessary to do it on their own.

But an MDR provider is only as good as the people, processes and technologies they use. So while they may help in many ways, there are key operational challenges that impact a provider's ability to deliver comprehensive detection and response capabilities at an affordable cost.

Many MDR providers have limited visibility into their detection processes, notifying you when a threat has been fully investigated, with little insight into what they're are doing to protect your environment in the moment. And if you are unable to track investigations and cases that are in process, your ability to respond may be delayed until you finally receive an alert from your provider.

Many MDR providers also only support limited detection technologies, either specializing on a small subset of data and leaving you blind to many attack vectors. In many cases they require you to deploy their preferred security stack, devaluing prior investments. And while human expertise is still critical, many MDR providers rely heavily on analyst activity for too much of the investigation process. Manual processes combined with a lack of visibility can lead to missing event context and incomplete case data, slowing your ability to effectively respond to threats.

Finally, one of the biggest shortcomings of many MDR providers (and almost all MSSPs) is a limited response capability. Many confine their responses to delivering recommendations that still require you to manually perform any incident response actions on your own, slowing MTTR. And while others have basic automation or human intervention available, they're overly dependent on variable analysis, making it difficult to confidently automate or hand over critical aspects of the incident response process.

In order to overcome these limitations, an MDR or MSS provider needs to find ways of delivering adaptable, accurate, and rapid services in ways that best meet the needs of their customers. The best way to do this is through an automation-driven approach to detection and response.

REASON
1

Automated Analysis, Investigation, Triage and Detection

Detection is one of the first, and often most difficult, steps in the threat management lifecycle. There are specialized security tools and platforms that analyze data from every angle, but the sheer volume of potential threats and the alert overload generated by those solutions can make identifying real attacks buried among the false positives an almost insurmountable task. But many MDRs still rely on security analysts to perform the bulk of the investigation process, leading to slow and inconsistent detection.

And the longer detection takes, the higher the risk to your organization. Automation is a critical tool for any MDR to get through the high volume of data necessary to deliver adequate detection capabilities. Automated detection playbooks allow them to analyze security event data and alerts at scale, rapidly detecting and triaging critical threats and delivering confirmed, true positives to security analysts for validation in a fraction of the time, saving countless FTE hours. This ensures that analysts (and you) will receive critical threat context and details faster, with a significant reduction in mean time to detect (MTTD).

"Receive critical threat context and details faster."

Things to ask your prospective MDR provider:

- Is the provider able to analyze, investigate and triage all security event and alert data at machine speeds?
- Will you have access to the platform used by the MDR provider for transparency into how analysis and detection playbooks are architected and implemented?
- Can your MDR provider collect, analyze, investigate and triage data from every applicable source?

REASON
2

Accurate and Repeatable Outcomes

The accuracy of your provider's detection and response services shouldn't be dependent on the inherent biases and differing skillsets that exist between the different individual analysts staffing their SOC. Security analysts are skilled at investigating and verifying threats and providing recommendations for the correct response. But no matter how skilled they are, it's unrealistic to expect them to deliver the correct assessment with consistent and accurate documentation for each and every potential threat. Particularly with the speed necessary to keep up with the high volume of security events and alerts generated every day. While many MDRs use automation for data reduction and alert triage, they still rely on security analysts to perform the bulk of the investigation process, leading to unnecessarily slow and/or inaccurate detections, inconsistent case documentation and notes, and mistakes in recommended responses.

Automation-driven detection and response follows the same, expert-defined process for analyzing, investigating and resolving threats at machine speeds. This gives SOC analysts faster access to critical threat details so that when expert intervention is needed, they can focus on confirming true positives. It also reduces the likelihood of mistakes tied to human error, formally documenting and following correct procedures and retaining tribal knowledge if and when analysts leave. And automation can be mapped to industry best practices like the MITRE ATT&CK framework, ensuring that consistent processes are followed so that all incidents are responded to in the right way every time, regardless of which analyst has been assigned to them.

"Consistant processes ensure that the same type of incident is responded to in the right way."

Things to ask your prospective MDR provider:

- How will your provider ensure consistency in investigation processes, detection reporting, and recommended actions between analysts?
- What capabilities will you have to measure your provider's response consistency over time?
- Does your provider map detection and response processes to industry best practices like the MITRE ATT&CK framework?

REASON
3

Immediate Response

A typical MDR provider's response capability is limited to performing basic actions or providing suggestions for your analysts to respond on their own, which may work in the many instances, but can limit your ability to immediately respond when you need it most. Most lack the automation tools necessary to perform actions in a way that adheres to your policies and operating requirements, and they don't want the liability of physically taking action on your behalf. This delays incident resolution because of the unnecessary gap between detection and response while your analysts wait for the provider to deliver event context. Executing the right actions in response to MDR-provided recommendations typically involves logging into multiple systems, creating additional delays in resolution. And with the destructive speed of many advanced attacks, every second counts.

Automation-driven response lets your provider build and orchestrate the right incident response processes and associated actions for specific threats using playbooks that work with your existing security stack. That allows you to perform immediate resolution in a way that adapts to your people, process and technology, while also adhering to your operating requirements and policies. A best practices approach includes options for deciding whether to execute actions automatically or queuing them up for immediate execution pending analyst approval. That delivers the most flexible means of reducing resolution times without violating policy.

"Perform immediate resolution in a way that adapts to your people, processes and technology."

Things to ask your prospective MDR provider:

- What capabilities does the provider have to execute appropriate actions automatically?
- If the provider does offer automated response, how many different actions and on what platforms?
- Does your provider's automation give you the flexibility to require human approval before execution?
- Does your provider's human approval process integrate with your existing and preferred communication channels (Slack, SMS, email, etc.)?

REASON
4

Operational Scalability

MDRs exist to help security operations teams overcome resource constraints, but without the right technology in place, they face the same operational issues as their customers. And these issues can be compounded for MDRs because they're performing these tasks for many different customers at the same time. Without automation they can't scale their operations as a provider, leading to resource constraints as they add new customers or deal with outbreaks. This can negatively impact their ability to detect and investigate threats, notify you of true positives, and provide recommendations for how to respond. Most MDRs use a combination of platforms to help with the process, but homegrown solutions for data reduction and basic triage don't manage enough of the process. Tools to perform basic automation or even enterprise SOAR platforms that can execute more complex playbooks, are often dependent on either human analysts or overly specific 3rd party event triggers to initiate the initial detection and response process.

For true operational scalability, automation is most effective when deployed in a single platform that orchestrates and automates both detection and response. This allows the provider's analysts to work in one place, managing each incident from start to finish without having to bounce between tools. Because the bulk of the repetitive, previously manual tasks are automated, they are only required to investigate validated true positives, which they can do in a single, consolidated case view. This allows each analyst to investigate and verify more threats, significantly extending their coverage capabilities. The same analysts are then freed up to build new automated playbooks that support multiple customer environments, expanding their reach even further. When response approval or additional actions are required, you're working with the same set of data, giving you complete transparency into the process from start to finish.

Things to ask your prospective MDR provider:

- What technologies is the provider using to empower their own analysts to overcome alarm fatigue and burnout?
- How will your provider ensure that their SOC is capable of keeping up with high volume alerts during periods of peak activities, significant outbreaks and after hours?

REASON
5

Process Transparency

The reason organizations engage with MDR providers is to help overcome the resource constraints that lead to alarm fatigue and analyst burnout, and also limit the ability to effectively deliver 24x7 security coverages. But having someone else manage specific aspects of your security operations doesn't remove the need for visibility into what is happening or how it's being done. Yet most MDR providers are limited in their ability to deliver visibility into what they are doing, because their tools aren't designed to effectively show how processes are built or followed. And because much of the detection process can vary from analyst to analyst, each case may be investigated in a different way. That leaves you with no real insight into what is being done until the investigation is completed.

When an MDR uses automated playbooks to perform the majority of detection and response activities, you can see exactly how threat detection and incident response will be performed for specific use cases and work with them to make any necessary adaptations to your requirements. That way you know what steps the provider will be taking to protect your organization, giving you both the assurances that you need and the insight to assess and address any potential gaps in coverages. And when automation is used, every followed process and action taken is automatically updated and displayed. That gives you visibility into exactly what is happening when it's happening, so that you can stay on top of any incident without surprises or gaps in knowledge. And automation makes it easier to record exact details about what actions have been taken, when they were taken, and how long they took to execute.

"Visibility into what is happening, when it's happening."

Things to ask your prospective MDR provider:

- Will you be given visibility into their analysis and detection rules to see how exactly investigations and triage will be performed?
- Will you be given portal views that show you what is happening when it's happening at every stage of the detection and response process?
- Will you be able to track and measure exactly how detection and response are executed?

REASON
6

Proactive, Continuous Threat Hunting

One of the benefits of engaging with an MDR provider is that it frees up your security team to spend time on more strategic and proactive security initiatives like threat hunting, in many cases in collaboration with the provider. However, the number of potential variables including multiple steps and tools, involved in executing each particular use case means threat hunting is typically a time consuming and manual process. And that's assuming that you know what to look for and how. The manual nature of threat hunting limits how frequently it can be done, so unless indicators of a particular threat are present at the time hunting is performed, it ends up being a time-consuming activity with minimal efficacy.

Automation is a powerful tool for running an effective threat hunting program. Playbooks that can automate previously manual processes are faster and more consistent, and they can be run on a near continuous basis to ensure greater success. Having access to the same platform as your MDR provider, with guidance from expert resources who already know your environment, is invaluable. And playbooks can be shared between similar deployments, delivering a proactive form of herd immunity as effective threat hunting programs act as a force multiplier across multiple environments. This is particularly powerful when combined with a provider's expert resources.

"A proactive form of herd immunity as when effective threat hunting programs act as a force multiplier across multiple environments."

Things to ask your prospective MDR provider:

- Can your provider perform continuous threat hunting via automated playbooks?
- Will your provider work with you to create relevant threat hunting playbooks that map to your environment and requirements as a standard component of their service offering?
- Will your security team have access to the same tools to create and execute their own threat hunting playbooks?

REASON
7

Customized Solutions

One size fits all doesn't work in cyber security. Each organization has a unique combination of people, processes and technology, with individual priorities and operating requirements. Yet because they are overly dependent on inefficient, human-driven processes and limited tech stacks, few MDR providers are equipped to adapt to their customer's needs. Instead, they require you to adopt or purchase specific technologies and rely on potentially limited detection and response processes and homegrown platforms that are designed to help the MDR provider operate at scale rather than meet your requirements. On top of that, you're restricted to specific provider-created dashboards and reports, limiting your ability to look at and analyze program efficacy or use the data in ways that are useful to you beyond basic detection and response.

Providers using an automation-driven approach to detection and response have the flexibility to deliver more customized solutions for you by integrating with your existing SIEM, EDR, NGAV, NGFW, trouble ticketing platform, cloud infrastructure, and any other technologies you have. Automated playbooks can be created and modified during onboarding and on an ongoing basis, to map to your organization, typically with minimal effort. Because the provider's automated playbooks handle the majority of time consuming, repetitive work tied to detection and response, their SOC is operating from a consistent set of data, without the typical overhead. Custom playbooks and dashboards have little impact in the way that they operate, allowing them to deliver flexible

"Automated playbooks handle the majority of time-consuming, repetitive work."

Things to ask your prospective MDR provider:

- Do they have the ability to customize their services to automatically collect, analyze, investigate and triage threats using your technology and preferred processes?
- Will they work with you to help build customized incident response playbooks to address specific use cases?
- Can they deliver custom dashboards and reports to deliver the information that you want and need in the way that you need it?

REASON
8

Continually Updated Content

Detection and response solutions are only as good as the expertise driving them. While that begins with the skill and training of individual security staff, relying completely on the applied efforts of individual analysts is inconsistent, doesn't scale, and leads to an ongoing loss of tribal knowledge with the inevitable staff turnover that every organization faces. Without access to expert content driving repeatable and consistent operations, an MDR provider will run into the same issues as the companies they're supposed to be helping.

Automation platforms allow MDR providers to deliver repeatable, scalable solutions in the form of playbooks, integrations, dashboards, reports and other expert content. This includes content that is deployment specific as well as sharable content delivering herd immunity through collective expertise. Automation also allows providers to more effectively create and deliver programs that map operations to best practice methodologies like the MITRE ATT&CK framework at scale. This gives you the assurance that your provider is delivering the highest quality detection and response on a continuous basis. And a provider who is developing new content on your behalf can effectively future proof your detection and response by creating new content no matter what you change in your environment.

"More effectively create and deliver programs that map operations to best practice methodologies like the MITRE ATT&CK framework."

Things to ask your prospective MDR provider:

- Will they be continuously updating detection and response content to ensure that you are protected from new threats using best practices?
- How do they ensure that they will continue to deliver a high level of service despite operational changes, including staff turnover (yours or theirs), new security solutions, and evolving attacker techniques?

THE LOGICHUB MDR+ DIFFERENCE

So what is it that truly differentiates LogicHub's automation-driven MDR+ from traditional managed detection and response?

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.

LogicHub's 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 ensure a best practices approach to detection and response at all times.

Our SOC analysts not only deliver 24x7 expert services, they continually work with you to create and update integrations, playbooks and other product content that ensures you're protected at all times. 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.

And we integrate with your entire tech stack, providing complete visibility while letting you keep the solutions you prefer and retain your previous investment. Any tools that we don't currently integrate with, we'll add in under two weeks at no charge to you.

Whatever your organization looks like, we deliver detection and response solutions that adapt to fit your requirements. And we'll continue to adapt and grow with you as those needs change, no matter what, delivering deeper detection, faster response, and lower dwell times.

LogicHub

301 N Whisman Rd Mountain View, CA 94043
info@logicHub.com • tel 650- 262-3756
logichub.com