LMNTRIX

BE THE HUNTER I NOT THE PREY

A Buyer's Guide

How to Select an MDR Provider?

Questions to Ask & Pitfalls to Avoid

Executive Summary

Cyber attackers have been enjoying an advantage over enterprises ever since digital assets have become as important as physical resources. The ever-increasing proliferation of digital technologies results in even novice black-hat hackers being able to plant ransomware on corporate servers and endpoints or yet launch a successful Distributed-Denial-of-Service (DDoS) attack against a corporate website.

Data protection and access to sensitive data are now at the core of any digitization strategy as information about a product is as valuable as the product itself. Digitization of data is an irreversible process across all industry verticals while all these piles of sensitive information need protection in regard to data access, data alteration as well as protection against unauthorized access to corporate networks on which data resides.

Modern technology and digital transformation as a whole introduce efficiency and simplify complex business processes but also create new attack vectors for bad actors to exploit when looking out for ways to compromize organizations' digital assets. Enterprise attack surfaces now broach upon new and largely untested areas of cyber-security which include the growing adoption of mobile devices used to connect to corporate networks, the widespread adoption of Bring-Your-Own-Device (BYOD) policies, the increase of the number of employees working from home as well as on the emergence of Internet of Things (IoT) networks as an integral element of an office or a manufacturing IT ecosystem.

This sprawling digital footprint is where attackers are finding one of their most significant advantages.

Bad actors only need to be successful in one of their penetration attempts to completely compromise an enterprise network. With more and more business-critical elements being connected to the Internet and other networks, finding a way in is just a matter of time where cyber defenses are missing or inadequate.

A determined attacker will always find a way in and targeted cyber-attacks succeed in more cases than one might imagine. An alarming trend is that while in the past victims of sophisticated cyber-attacks were large enterprises and multinational corporations, now bad actors are also targeting an increasing number of small and medium-sized enterprises.
The bad news is that bad actors are gaining additional advantages both over the increased attack surface and the widespread use of traditional defensive strategies that are no longer effective. Enterprises fall victim to their own overly optimistic approach. In thinking they could completely secure their environments within a highly interconnected world, they sometimes use outdated models to solve a modern problem.

Obviously such an approach does not work.

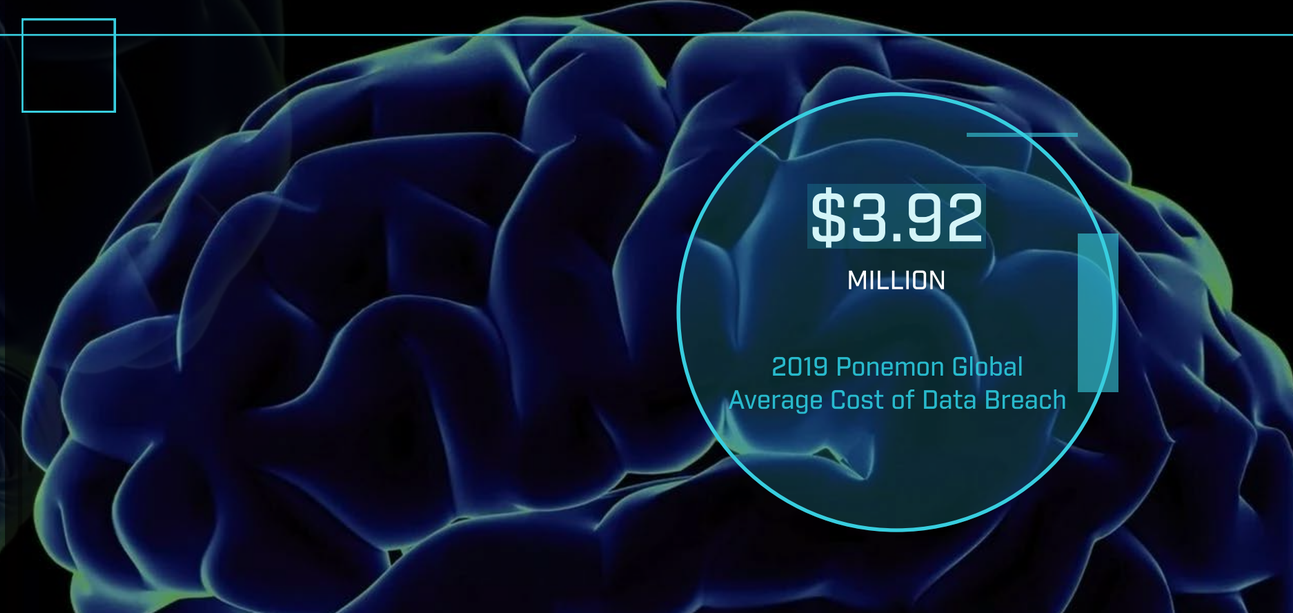
A number of organizations are now looking to fortify their frontiers, focusing on the perimeter. This reasoning does not work in the context of the connect-to-everything model as you can hardly build an efficient business ecosystem that is isolated from the outside world. Furthermore, when defenses are looking outward, you are obviously less capable of detecting an intruder once he/she has managed to enter the inner perimeter.

This false sense of security gives an attacker all the time in the world if the external-perimeter alarms fail to activate. While you might be thinking you are safe, an intruder might already be inside your network, moving carefully and spending months to finally get access to your most sensitive data.

There is no point in delving into a bad actor's motivation: it might be they are after intellectual property, or else might want to lay a hand on personal data about your customers, or might be seeking to completely destroy your digital operations. The greater problem is that whatever the motivation of an intruder might be, you should be able to identify and stop such intrusions as they occur and not after the damage is done. Which in turn requires an adequate and pro-active model of cyber-defenses that also detects unknown threats and abnormal behavior as opposed to the old-school model of threat detection that relies mostly on virus signatures and detection of already known malware.

Managed Detection and Response (MDR) reimagines cyber security. It takes the traditional security mindset and turns it on its head. By realizing that an enterprise's digital borders can never be completely secure, it turns the attention inward and, in doing so, it turns the tables on attackers.

By focusing on the detection of attacks that breach the perimeter, you can rapidly recognize and respond to breaches. This significantly reduces the time an attacker can spend within your network and minimizes a bad actor's ability to do material harm.



Introduction

The threat landscape is increasingly complex and dynamic. Adversaries are well-funded, resolute and innovative in creating new tools and techniques to advance their mission. Enterprises quickly learn that their Security Operations Center (SOC) or investment in advanced technology alone will not stop determined malicious actors.

The problem is that when organizations try to outsource managed security, vendors often do not meet expectations:

- Organizations either experience breaches under the watchful eye of a managed security vendor or they realize that they do not detect anything when they run a Red Team exercise.
- Threat detection capabilities of traditional Managed Security Service Providers (MSSPs) are primarily limited to monitoring logs and identifying known threats. The focus is on preventing intruders from entering the network, but once such an intruder penetrates the network perimeter, ongoing malicious activities
go completely undetected.
- Traditional MSSP services, which are designed to provide cost-effective compliance and device management capabilities, in fact detract the vendors from risk mitigation efforts as they mostly overemphasize alert management.
- When an organization enhances or upgrades its security infrastructure, outsourcing costs can increase dramatically based on the additional number of sites, personnel and endpoints.
- Most managed security service providers play the role of tier one analysts focused on alert validation and notification, rather than on decreasing an attacker's dwell time — the amount of time a bad actor spends in your environment.

The managed detection and response (MDR) approach addresses the need for real-time threat detection and response. It also eliminates the above shortcomings of the legacy approach to managed security. And since each vendor takes a different approach to running and delivering services, you need to determine how a specific approach will protect your organization.

This paper helps you identify and evaluate the most critical capabilities of MDR service providers and offers a checklist of pertinent questions aimed at assessing a prospective vendor's approach while avoiding common pitfalls. By taking advantage of our guide, you can make an informed security investment decision and effectively protect your organization against various cyber threats.

Questions to Ask

What Makes Up Your Technology Stack?

A comprehensive technology review can help you assess how extensive and potentially effective the threat detection abilities of the MDR provider can be. This will allow you to qualify them in/out early in the evaluation process.

Many of the MDR solutions currently on the market focus on single-security technology, such as Endpoint Detection and Response (EDR) which makes them actually a provider of the managed EDR service and not a true MDR. This seriously restricts the exposure of the service provider to many threat vectors including network born and encrypted attacks as well as lateral movement. Furthermore, their post-breach forensics capability is limited to information from endpoints, leaving them with insufficient evidence to tell you the full story behind a breach.

Organizations should look for an MDR solution that offers capabilities such as behavioral analytics, incident forensics, breach response, network and host-based intrusion detection, adaptive and distributed deception architecture for fending attackers off. Such a solution should also utilize extensive threat intelligence capabilities within the platform. The solution should have functionality such as advanced behavioral analytics for detecting anomalies on the network and on endpoints, as well as deep- and dark-web monitoring to understand what the shady sections of the world wide web know about the organization and its digital assets.

A solution featuring such a variety of modules is capable of maintaining full coverage of the attack surface while early detection helps minimize false-positive alerts. It also enables security analysts to quickly gain significant threat context during an investigation, resulting in a faster time to containment, remediation and attribution.

Gartner's definition for an MDR provider includes the delivery of services using the vendor's curated technology stack to free customers from the burden of selecting and maintaining protection technology. MDR providers should also use what they learn from protecting their customers' environments to improve the technologies they deploy.

Legacy providers of managed security services typically spend their time correlating logs from hundreds of products that limits them to signature-based detection. They do not tell you anything you do not already know. An effective MDR provider correlates information from multiple layers of detection analytics, systematic analyst-driven hunting processes and supplementary network and endpoint evidence to reveal anomalous activity at each stage of the attack lifecycle.

By using a consistent technology stack for every customer, MDR providers can build up large datasets on alerts, contextual actions taken and investigative decisions implemented. These analyst decisions become another source of knowledge that can be applied to continuously improve the efficacy of the associated technology products. When analysts' hunting activities identify changes in attacker's Tactics, Techniques and Procedures (TTP), such insights should be quickly transformed into new product detection capabilities and Indicators of Compromise (IOC).

If you manage to find an MDR with limited intellectual capital (e.g. technology innovation, threat hunting, anomaly detection, intelligence, etc.) who is simply managing another vendor's tool set such as an EDR or a network sensor, or using open source technology and collecting logs and calling themselves an MDR, you should reconsider your decision to hire them. These are activities you can well perform in-house, i.e. such an MDR provider will hardly add much value to your overall security. In this case, doing it in-house will deliver a far better outcome as you will be more focused and will know your own assets, your data, your people, and you will have context around the alerts you receive when compared to an external MDR that has no knowledge about any of these things.

BLIND SPOTS IN THREAT DETECTION & RESPONSE

24%	8%	11%
Have Visibility into Attacks	Can Quickly Detect Attacks	Can Quickly Investigate Attacks

LMNTRIX
Survey of 350 Global Enterprises

Questions to Ask a Prospective MDR Provider:

1. What makes up your technology stack?
2. What is your post-breach strategy for detecting malware that has bypassed our perimeter controls?
3. What is your post-breach strategy for detecting human adversaries that have a point of breach and are looking to move laterally?
4. What is your strategy for detecting encrypted attacks?
5. What is your strategy for detecting insider threats?
6. What is your strategy for detecting unknown threats?
7. What is your post-breach forensics capability? And how long do you keep the evidence?
8. How do you transform changes in the threat landscape into product and technology innovations that result in better detections? Provide recent evidence of such innovations.
9. As an MDR vendor, how do you maintain your cyber-security domain expertise?

Questions to Ask

What Makes Up Your Platform?

Your organization should look for an MDR provider that demonstrates significant intellectual capital around their platform. Ideally, their platform should provide you with an overview of your entire network and the ability to respond to the highest priority threats via deep forensics and powerful collaboration tools.

You should be looking for MDR vendors with platforms that allow them to offer behavioral analytics, unlimited retention window of full-fidelity network traffic, innovative security visualizations, pervasive visibility, threat hunting, intelligence, validation, investigation, containment, remediation and unlimited forensic exploration on-demand. Platforms that offer integration with third-party controls such as NG Firewalls as well as cloud security providers such as Zscaler, Cisco Umbrella and Infoblox for automated threat containment should be looked at favorably as they expedite the threat containment process while reducing your team's overhead. Make sure that they can show and demonstrate their platforms, and ideally you should be able to have access to the same capabilities.

MSSPs adopt the traditional log-based approach to threat detection that has failed the industry for more than 20 years. If the MDR vendor relies solely on logs and Security Information and Event Management (SIEM) for their platform, then they are nothing more than an MSSP disguised as an MDR. You should take caution when considering such vendors and ensure that you test their claims of efficacy thoroughly before making a buy decision (preferably by thoroughly comparing them to the service and capabilities on offer from several other MDR providers).

Questions to Ask a Prospective MDR Provider:

1. What makes up your platform?
2. Does your platform provide behavioral analytics and machine learning for uncovering advanced and unknown threats? If so, provide details.
3. What visibility to threats does your platform provide us in real-time?
4. Does your platform provide us access to your threat hunts and hunt results?
5. Does your platform allow us to validate, investigate, contain and remediate incidents?
6. What kind of data do you collect from our network and applications?
7. How long do you retain the data that you collect from us?
8. Does your platform provide us access to full-fidelity network traffic with unlimited forensic exploration on-demand?
9. Can we have a demonstration of your platform?
10. Do you collect logs from our network and do you use a SIEM for detecting threats?
11. What third-party integrations does your platform offer for automated containment?

A LOGS-ONLY APPROACH TO DETECTION ISN'T WORKING

83%
Percent of incidents that not took weeks or more to discover

99%
Percent of successful attacks went undiscovered by logs

LMNTRIX
Survey of 350 Global Enterprises

Questions to Ask

Will the Service Provide Visibility for Cloud Assets?

As organizations increasingly move to cloud infrastructures, securing these environments is the most recent cyber-security challenge. Organizations must have the ability to monitor critical resources whether they are in the server farm or the cloud and MDR vendors should be able to expand their services to cover such hybrid environments. MDR vendors that cannot support such environments would pose a challenge to organizations' operations and most likely will add overhead in terms of cost and time to implement.

Even if your organization is currently not using the cloud, it is wise to evaluate MDR vendors based on their preparedness to help your future cloud migration. This will save you time and money in the long-term. Thus, you should not be forced to change MDR vendors when you eventually decide to migrate to the cloud.

MDR vendors that offer native cloud monitoring for critical cloud resources should be kept into consideration, as these would integrate flawlessly with the vendor's security monitoring service. The ability of the service to benchmark your security posture in the cloud is an added benefit. This would help your organization improve the shortcomings in your security policies and help the vendor focus on monitoring and hunting for threats.

Questions to Ask a Prospective MDR Provider:

1. Does your solution extend to the cloud (we use "xxx" for our cloud)?
2. Does your entire technology stack support the cloud – if not, what are the limitations?
3. Does your solution provide visibility through a single interface across both enterprise and cloud assets?
4. Do your endpoint and network containment features also work on the cloud?

Questions to Ask

Does the Vendor Provide Validation, Investigation, Containment and Remediation of Incidents?

No matter how good your security is, experiencing a breach is highly likely. A significant differentiator to the traditional managed security model and a critical outcome from an effective MDR vendor to reduce dwell-time is their ability to conduct validation, investigation, containment and remediation following a breach.

The vendor should take special care while onboarding a customer to understand their environment, baseline the findings and tune their technology stack, to help reduce the noise. Each alert that is raised should be extensively validated and investigated and provide attribution to threat actors where possible. The expertise of the team employed by the MDR vendor should be at par with the evolving nature of bad actors to effectively handle security threats.

MDR vendors differ based on their technology stack and the Service Level Agreements (SLA) they provide. Some vendors might only send alerts just like the traditional MSSPs, while others may provide recommendations along with incidents raised to your team and charge extra for any incident response. It is important to distinguish between vendors and the level of Incident Response they perform.

Effective and outcome-based MDR vendors would take control over an infected system quickly and isolate it from the network to perform advanced forensics to identify the tools, techniques and procedures (TTP) of the attack. They will also find indicators of compromise and create a detailed timeline of the attack before automatically containing and remediating threats to limit the scope of an infection or attack.

More than
90%
of our clients used an MSSP while they had a major breach.

Carlo Minassian
CEO LMNTRIX

Questions to Ask a Prospective MDR Provider:

1. What is the scope of your incident response following a breach?
2. What type of investigative actions do you provide?
3. What type of containment and remediation do you provide?
4. Provide examples of several incidents that demonstrate your incident response capability?

Every Second Counts after a Breach

Organizations need effective MDR vendors which can provide incident response service that can quickly contain affected systems and disable all known operational capabilities of the threat actor. The MDR vendor's incident response experts should immediately validate potential incidents, provide appropriate context, investigate as much as is feasible about the scope and severity, make recommendations and guide or suggest methodical remediation. After the investigation, orchestration tools should be employed to automate and accelerate response activities, further reducing dwell time and risks.

Lastly, when your organization has breach disclosure obligations, you can minimize loss and exposure if you have a complete picture of the compromise and the ability to pull in additional response resources.

Does the MDR Service Provide Proactive Threat Hunting?

The Proactive Threat Hunting service involves the proactive, stealthy, and methodical pursuit and eviction of adversaries that may already be in your network – all without relying on Indicators of Compromise (IOCs).

Traditional defenses cannot keep up with new attacker techniques, leaving companies vulnerable to hacks. Even if the good guys could match their adversaries' offensive tactics, there would still be times when their defenses would fail. It is quite probable that an employee will click on a malicious link in an email, or will visit a compromised website, or a firewall will be improperly configured.

Unlike traditional, reactive approaches to detection, threat hunting is proactive. With threat hunting, security professionals do not wait to take action until they have received a security alert or, even worse, suffer a data breach.

Instead, threat hunting entails looking for opponents who are already in your environment. Hunting leads to discovering undesirable activity in your environment and using this information to improve your security posture. These discoveries happen on the security team's terms, not the attacker's. Rather than launching an investigation after receiving an alert, security teams can hunt for threats when their environment is calm, instead of doing so in the midst of the chaos that follows when you detect a breach.

Threat hunting is often used by MDR vendors only as a selling point, therefore you need to carefully evaluatethe vendor to understand their capabilities. Ideally, an MDR vendor would provide a mature threat-hunting service that follows a detailed process while they are continuously evolving their hunting process to look for threats either specific to current IT ecosystems or tracking an adversary that is dynamically changing its attack infrastructure to infect and compromise new organizations.

Proactive threat hunting is a core competency of any MDR. If the MDR vendor is weak in this area, then the outcome and ultimate value they are going to deliver is minimal. Watch out for MDRs that run searches using IOCs and call this technique threat hunting, as this is not the real thing.

$1.27

million dollars wasted responding to erroneous or inaccurate malware alerts

2017 Ponemon Global Average Cost of Data Breach

Questions to Ask a Prospective MDR Provider:

1. Provide details of your proactive threat hunting capability?
2. If your hunting includes more than just IOC searches, provide detailed evidence.
3. How often do you hunt for threats?
4. Does your threat hunting include both endpoint and network data? Please show us 20 examples for each.
5. Do you provide automated threat hunting and if so, provide details?
6. How do you use your hunting outcomes to better develop and improve your technology stack and platform development?

Questions to Ask

Is the MDR Solution Intelligence Driven and Context Aware?

Threat intelligence is another core competency of any MDR. It is an important factor that provides a vendor with necessary information about new threats to make informed decisions on employing new threat hunting techniques and focus on TTPs for detection, investigation, and response.

The quality of threat intelligence feeds also impacts the output of the service. MDR vendors often accept threat intelligence data from the clients and then incorporate it in their service. Vendors that take inputs from a variety of threat intelligence sources, including deep and dark web intelligence, would perform better on average. Additional points should be given to vendors that are taking inputs from intelligence organizations such as the law enforcement, national defense agencies or CERTs (Centers for Incident Response in Information Security) because this signifies the capability to detect state-sponsored threats with more confidence.

> “Know your enemy, know his sword”
>
> «Miyamoto Musashi»

Questions to Ask a Prospective MDR Provider:

1. How do you use threat intelligence to update the service?
2. Do you produce your own intelligence?
3. What and how many intelligence sources and threat feeds do you use?
4. Can I integrate my intelligence sources with your platform?
5. Do you use attacker playbooks and if so, how quickly do you update them?
6. Is the solution context-aware and if so, provide details of how you achieve this? For example, how do you integrate context with network data?
7. Does your intelligence give us an indication of who could be behind an attack? Please provide examples.
8. How quickly can you apply intelligence gained from other clients to our environment and what is the process you use for this?
9. Do you conduct your own research to inform your intelligence and if so please provide 10 examples of such research?
10. Can we have access to your intelligence via your platform?

What is the level of Investigation and Incident Reporting?

Because traditional MSSPs lack any proprietary technology stack, they simply rely on collecting logs from the organization's existing security controls. As a result, the coverage of their service is limited to rapid alert notification, limiting the MSSPs' role to a tier one analyst who simply passes alerts to the client.

In this capacity, they are nothing more than a very expensive messenger for your existing security controls. This typically leaves organizations frustrated and surprised to what they signed up to as they are left dealing with an overwhelming number of notifications with no understanding of the probable identity or motivations of threat actors.

As per the contract the organization signed up to, the MSSP has met their 10-min SLA of passing anything that comes their way and there is nothing the organization can do about it but to wait until their contract expires. In contrast, an effective MDR vendor will spend hours validating, investigating and documenting a threat before they take any containment and remediation actions.

With the traditional MSSP approach, providers prioritize speed of reporting over depth and context, and as a result the burden of validation and investigation lies with the client. Instead of focusing on higher-order activities that ultimately reduce attacker dwell time, the client's security team ends up spending an excessive amount of time running down false positives and rudimentary alerts.

Opposite to that, effective MDR vendors provide answers, not alerts. They fundamentally reject the use of a SIEM, and they also reject a log-based approach as a starting point for real-time threat detection and response. Although device alerting is still useful as supplementary evidence during investigations, effective MDR providers rely on a proprietary technology stack and a platform that supports the entire life cycle of the security operations workflow - from analyst-driven, intelligence-led and context-aware based detection through investigation to response.

Effective MDR vendors exclusively rely on an intelligence-led approach that combines analyst-driven detection with correlated incidents from a proprietary technology stack and platform to drive targeted investigations. MDR vendors combine extensive knowledge of specific threat groups' behavior with rigorous investigation methods to discover signs of intrusions, learn how attackers are operating and assess their capabilities. Throughout an investigation, outcome-oriented MDR vendors continually update their investigation reports to include the context needed for organizations to fully understand the scope of the attack as well as information to help assess risk and definitive remediation recommendations.

As a result, effective outcome-focused MDR vendors will deliver their clients on average, about a dozen validated incidents in any given month while the traditional MSSP continues to deliver hundreds and thousands of rudimentary alerts and false positives together with a monthly report that is generally filled with meaningless non-actionable statistics and graphs.

With any effective MDR vendor, the quality of service and the overall value they provide is largely determined from the Incident Reports that are handing over to you. The way the process of delivering these reports and the follow up communication are working determines how the vendor and your team will blend together in the long -term.

Vendors often communicate via custom incident portals and emails. Some vendors also provide communication channels via Slack, direct chat access to analysts or dedicated phone numbers to the technical team. Evaluate vendors based on how easy it is for your team to assimilate the Incident Report information and take necessary actions, if required. You need to have uninterrupted and easy communications for each incident and you should be able to maintain the overall communication this way.

Questions to Ask a Prospect MDR Provider:

1. How do you measure the effectiveness of your service?
2. What is the level of investigation and reporting that you provide?
3. What are the communication methods that your SOC supports with our team?
4. What type of reports do you provide?
5. What kind of information do you provide in addition to reporting alerts?
6. How effectively do your reports convey the context of a threat and associated details such as:
   - a. How did bad actors get in?
   - b. How long were they there?
   - c. How did they get around?
   - d. What tools did they use?
   - e. Did they setup any backdoors?
   - f. What data did they access/steal?
   - g. What are they doing with our data?
7. Do you deliver a monthly incidents summary report? Provide sample.
8. Do you provide a monthly detailed technical report? Provide sample.
9. Can we schedule reports?
10. Do you offer on-demand reports?
11. Can we see 10 examples of your incident reports covering the period before the incidents were closed?

Vendors That Depend Heavily on Log Collection

Vendors that depend on the collection of logs for most of their service output would deliver very little value and, in most cases, offer rudimentary threat detection and a false sense of security.

Such vendors perform analytics on the collected data which is often limited to static rules and signatures. These detection techniques are easily evaded by modern-day adversaries. An effective MDR vendor does not rely on the collection or storage of logs, but data about events and behaviors which they analyze based on advanced detection techniques employed using their own proprietary technology stack.

The MDR vendor should have minimal if any reliance on logs from your existing controls and they should not be using logs or a SIEM to deliver their solution. That is because if your controls know about a threat, they will block it.

Your existing cyber-security systems are supposed to not let known threats onto the network, so relying on their system logs to try and detect a threat is a pointless exercise. This is why so many enterprises with multi-million dollar SOC contracts and SIEM investments continue to get breached time and over again.

Following 20 years of adoptions, it is now well-known that log management and SIEM solutions are a failed commodity used to please compliance mandates and at best used for network troubleshooting. If you see a vendor try and sell you a SIEM-based MDR solution, we recommend that you seriously consider what you are investing in.

On the other hand, if you find a MDR vendor that delivers log management or SIEM capability for no extra cost, which complements a MDR service offering, then they are certainly worth looking into.

Vendors That Fail to Deliver Value during the Service Evaluation Phase

Make sure to evaluate vendors on their preparedness and ability to detect and respond to threats, after all that is what you are going to pay them for. It is highly recommended to involve a third party to perform Red Teaming (penetration testing) on your organization so as to set a specified goal for exfiltration of sensitive information. You should also conduct advanced persistent threat (APT) attacks, but without notifying the MDR vendor under scrutiny. This would test the declared Mean Time to Respond (MTTR) by the vendor and will also give you a sense of what to expect during times of an actual security breach or attack.

Regardless of how the vendor answers the questions in this document and by putting their claims aside, or their popular brand, or any analyst reports and magic quadrant placement, we urge you to do this one thing and test the vendor over a 30-day period.

In the ideal scenario, you will have several vendors providing test services on the basis of the very same data during the trial period. This is where the rubber meets the road and you're able to experience first-hand how the vendor's technology stack, platform and team perform in your unique environment. Naturally, you should choose the vendor that delivers the best outcome for you during this period above all else – and fire the ones that deliver nothing more than a high number of alerts or excuses!

Pitfalls to Avoid

Apart from the vendors' ability to perform security monitoring and investigations, it is also important to evaluate the ease of deployment of their sensors and how scalable these methods of deployment are. Consider the number of endpoints and network sensors that are needed to deploy and how much effort goes into deploying each sensor.

A vendor should have simple and scalable methods to deploy their network and endpoint sensors. The responsibility for maintaining and updating the sensors during the life cycle of the service should be clearly defined before you put pen to paper. These service details should be part of the evaluation of a vendor since your organization would not want to invest time and effort in the maintenance of the sensors but rather focus on dealing with incidents.

Vendors with Very Difficult Deployment Process and Lack Scalability

Vendors That Use Excessive Technical Jargon and Marketing Tricks to Compensate for Lack of Capability

Watch out for vendors that answer all your questions by saying that they use artificial intelligence (AI) or machine learning (ML). If the vendor's website has the term 'AI' everywhere, then you should be suspicious about them investing more in marketing initiatives rather than in developing their technology or service.

You can apply AI and ML to detect threats in a limited number of use-case scenarios , however it does not replace existing techniques such as Intrusion Detection, Threat Intelligence, Sandboxing, EDR, Bot Monitoring, Data Loss Prevention (DLP), etc. that are all very effective in detecting threats.

You can find numerous enterprises that experienced data breaches following a significant investment into building a SOC or contracting an MSSP that had very little detection and response capability but had managed to convince them otherwise with their fancy theatrical style facilities.

The people, processes, technology, automation and intellectual capital behind a SOC is far more important than the physical aesthetics of a SOC. So don't become part of the statistics that falls for the shiny SOC instead of the vendors' core competencies. Focus more on the end results you will get and what value the service delivers to your business. Make sure the MDR provider has the right team structure and capabilities in place combined with the right skills to operate a modern SOC.

Their team structure should at least include teams specializing in Threat Detection, Threat Response, Threat Hunting and Threat Intelligence. The skills you should look for amongst these teams include malware analysis, binary triage and analysis, Windows internals, Windows file system, Windows registry, intelligence research, open source research, programming/scripting, Intrusion Detection System (IDS) signature writing, netflow analysis, protocol analysis and forensics expertise.

Vendors with a Fancy SOC Facility to Compensate for Lack of Capability

Conclusion

Bad actors are getting better in their trade by the day and take advantage of increasingly sophisticated attack methods that evolve to avoid detection by the traditional log and compliance-oriented managed security services and alert-driven detection. To keep up with the challenges of modern cyber-security, enterprises need to go beyond basic alerting and chasing false-positives and recruit MDR providers that evolve just as quickly.

As new MDR vendors compete for mindshare and dollars with similar-sounding offerings, it can be difficult to distinguish which ones provide definitive detection and response capabilities. The criteria, questions and pitfalls outlined in this guide provide organizations with a toolset to understand and evaluate the available MDR options.

An effective outcome-oriented MDR provider blends technology with human expertise in tracking and spotting novel TTPs to validate, investigate, contain and remediate threats. Organizations should understand the importance of focusing on intelligence-driven and context-aware hunting, analytics, investigation and response using purpose-built technologies.

Your organization should only consider trusted MDR providers offering cyber-security solutions tailored to your specific needs. Every dollar spent on MDR services should translate directly into reduced business risks through demonstrable cyber-security improvements.

Make sure your MDR provider is up to the challenge.

By 2024

25%

of organizations will be using MDR services, up from less than 5% today.

40%

of midsize enterprises will use MDR as their only managed security service.

Gartner Market Guide for Managed Detection and Response Services
July 2019

About LMNTRIX Active Defense

LMNTRIX is a managed detection, investigation and response service that leverages industry-recognized cyber security expertise and threat intelligence to accelerate detection and investigation of cyber-attacks.

To learn more, visit lmntrix.com

LMNTRIX is the leader in intelligence led security-as-a-service. Working as a seamless, scalable extension of customer security operations, LMNTRIX offers a Gartner recognized MDR solution called Adaptive Threat Response that blends our cyber defense platform namely the LMNTRX Grid with an innovative security technology stack, nation-state grade threat intelligence and world-renowned Cyber Defense Centers. With this approach, LMNTRIX eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber-attacks.

LMNTRIX, Inc.

333 City Blvd West, Suite 1805, Orange, CA 92868 USA

+1.888.958.4555

info@lmntrix.com

lmntrix.com