White paper

A CISO's guide to selecting a managed detection and response partner

Rafeeq U. Rehman, Distinguished Architect

With the need for effective threat detection and response becoming more crucial by the day, cybersecurity leaders realize that partnering with a vendor is crucial. At the same time, they are confused about which service provider is right for their business. This white paper is intended to help you understand the essential components of a managed detection and response (MDR) service, as well as provide some criteria for identifying the right partner.

EDR, MDR or XDR

Detection and response terminology can be confusing. The industry currently uses three major acronyms, sometimes interchangeably:

1. **Endpoint detection and response**
   Endpoint detection and response (EDR) refers to platforms that focus on real-time endpoint monitoring and threat response. Many of these solutions have typically evolved from malware protection, installing an agent on the endpoint. They are managed from a centralized console where data is collected and stored, and administrators can perform tasks.
2. **Extended detection and response**
   Extended detection and response (XDR) solutions enable visibility beyond endpoints. This extended landscape may include telemetry data from networks (e.g., NetFlow), security devices, VPNs, email, cloud and other resources. They correlate data from these points of origin and provide options for a response from a central control point, typically a software-as-a-service (SaaS) platform or cloud.
3. **Managed detection and response**
   MDR is a category of services that EDR/XDR vendors or third parties provide using tools from different vendors. MDR service providers may use a combination of host and network-layer technologies, as well as advanced analytics, threat intelligence, forensic data and human expertise, for investigations, threat hunting and incident response.

Essential ingredients of any MDR solution

An effective MDR solution includes much more than technology and tools. Six ingredients are essential for the success of MDR and to fully realize its benefits.[1] If you miss any of these ingredients, the solution will eventually fall apart and fail to deliver its intended outcomes. Figure 1 shows the six ingredients, which, when combined with continuous improvement activities, help ensure the long-term success of the solution. The first thing you need to investigate is whether the service you're being offered is focused only on tools or is a combination of ingredients that brings the whole solution together using a good recipe.

The essential ingredients mentioned in Figure 1 include:

1. **People**
   A well-designed MDR service includes people with different levels of expertise in diverse areas, including networking, operating systems, applications, operations management, scripting, Python programming, vulnerability management, incident handling, forensics and more. A typical MDR service also includes a number of customer-facing roles that include advisory, technology management and service delivery.
2. **Security Operations Center processes**
   While there are many Security Operations Center (SOC) processes, effective incident detection and incident management is a key process for the success of every SOC. A SOC may also rely on other IT systems/processes like asset management, change management, patch management, etc.
3. **Governance**
   A well-defined governance structure enables MDR service management and continuous improvement while ensuring that business objectives of the MDR customers are achieved.
4. **Technology stack**
   Appropriate technology is needed for collecting log and other types of telemetry data, storing data, and processing/analyzing data. Main technologies used in MDR services

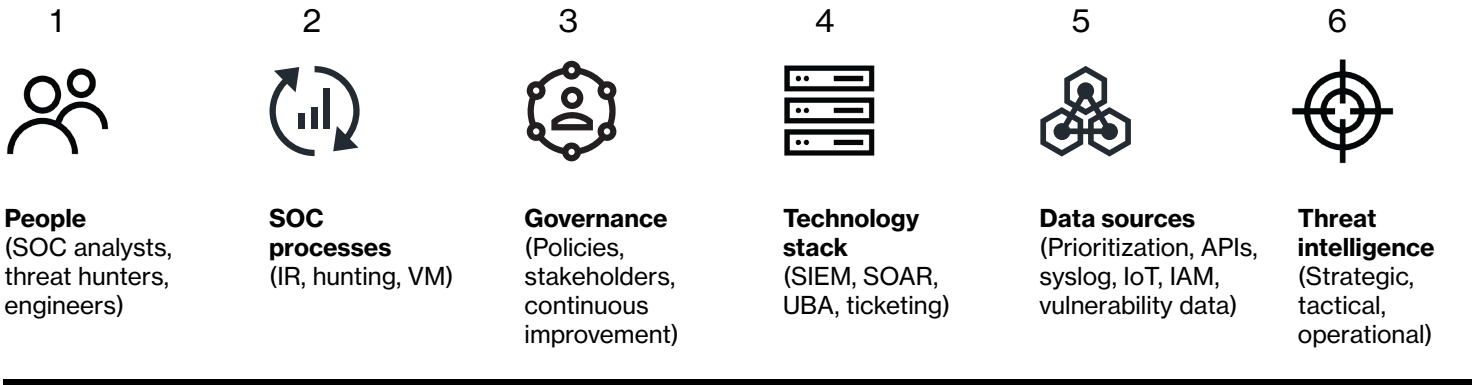

Figure 1: Essential components of MDR solution combined with continuous improvement activities

include a security information and event management (SIEM) tool, log collection infrastructure (syslog, application programming interfaces, etc.), network sensing, ticket/incident management, forensic tools and vulnerability management tools.

5. **Data sources**
   Carefully selected data sources provide high value in threat detection, investigations and response. Users need to be careful and selective in determining the type and amount of data that is fed into the technology stack. More is not always better.
6. **Threat intelligence**
   One of the key success ingredients of any MDR service is reliable and up-to-date threat intelligence. It helps in proactive threat hunting and automation, responding to threats at machine speed.

As you can see in the bottom part of Figure 1, just having the necessary ingredients of an MDR service will not suffice. A prospective service provider should work continuously on service improvement with a strategy that includes not only updating technology, but also having a plan for staff training and process improvement. This is a frequently overlooked aspect that results in the gradual decay in effectiveness of the MDR service.

Recommendations for selecting an MDR provider

Now that you have a better understanding of the necessary components of an MDR service, it's time to explore the selection of an MDR service provider that will serve your business objectives. One common practice is to invite vendors for presentations of their solutions. If you use that approach, ensure that the presentations are not limited only to technology and dashboard demos, but also provide information on key aspects of the service. Recommendations that you should consider when selecting a particular MDR service provider include:

Recommendation 1: Expertise and a focus on outcomes, not on technologies and tools

In Bruce Schneier's words, "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."[2] An MDR service is not about tools and technologies. It's a comprehensive solution that has many essential features and components to enable effective risk management. When considering an MDR service, you should focus on the service provider's expertise and business outcome delivery. Expertise covers the people, processes and governance aspects of any MDR service. Technology, no matter how advanced, is not effective unless it's coupled with mature processes for running a 24/7 SOC, threat intelligence, response capabilities and a sound governance structure that ensure continuous improvements to the service.

Recommendation 2: Automation and the transition of work to machines

Attacks happen at machine speed. Many attacks are customized and hard to detect using traditional correlation methods. You need to make sure that attacker capabilities are matched with detection capabilities at the machine level for identification of patterns, anomalies, user behavior, endpoint behavior and automation. On top of human capabilities, explore how your MDR service provider is using machine learning capabilities to identify newer attacks and anomalous behavior.

Recommendation 3: Visibility where it's needed (endpoints, cloud, IoT, network traffic, deception)

Every organization is on a digital transformation journey, although at different stages. An essential aspect of digital transformation is the use of new technologies and processes that include, but are not limited to, agile development, DevOps, cloud, IoT, machine learning and so on. Visibility at endpoints is no longer sufficient for the early detection of threats. Telemetry data and signals coming from different sources are no longer limited to syslog. It is essential that the MDR service provider is capable of receiving signals at least from the following sources:

- Endpoint security technologies
- Cloud services using application programming interfaces (APIs)
- Network traffic, either full packet capture or NetFlows
- Deception technologies

The MDR service provider includes advisory services to provide you with guidance on which signals matter more and how to balance the cost of storing/processing data.

Recommendation 4: Flexibility in service customization with optional components

An overall MDR strategy has many components and a chief information security officer (CISO) may not want to implement all of these components right from the beginning. Your MDR service provider should be able to offer you a foundational service package coupled with options to add more components as your program matures.

Recommendation 5: Proactive threat hunting

No matter how sophisticated the detection technologies are, some threats will be successful in evading detection methods. Proactive threat hunting, as part of MDR services, is a necessary component to search for anomalies and patterns that are questionable and need explanation. Threat hunters look deeper into data to formulate threat hunting hypotheses. Threat hunters also use threat intelligence feeds and their knowledge of the overall threat landscape to build and improve their monthly threat hunting strategy. The main thing you need to do is make sure that your MDR service includes a threat hunting component that is not optional.

Recommendation 6: Support for multiple EDR solutions

You may have one EDR solution today but want to change it down the road. Even if you don't plan to change your EDR solution in the near future, you may acquire a company that has a different EDR than you have. Your MDR service provider shouldn't lock you into a specific EDR solution and should be able to work with what you already have, as well as support a different or even multiple EDR solutions, in case you become engaged in merger and acquisitions activity.

Recommendation 7: Program management with feedback loop

An MDR strategy includes a strong collaboration and partnership between you and your MDR service provider. A programmatic approach to an MDR solution should enable collaboration, idea sharing and a feedback loop from both sides through a service advisor who has regular meetings with your team, provides updates and becomes your voice to the MDR service provider.

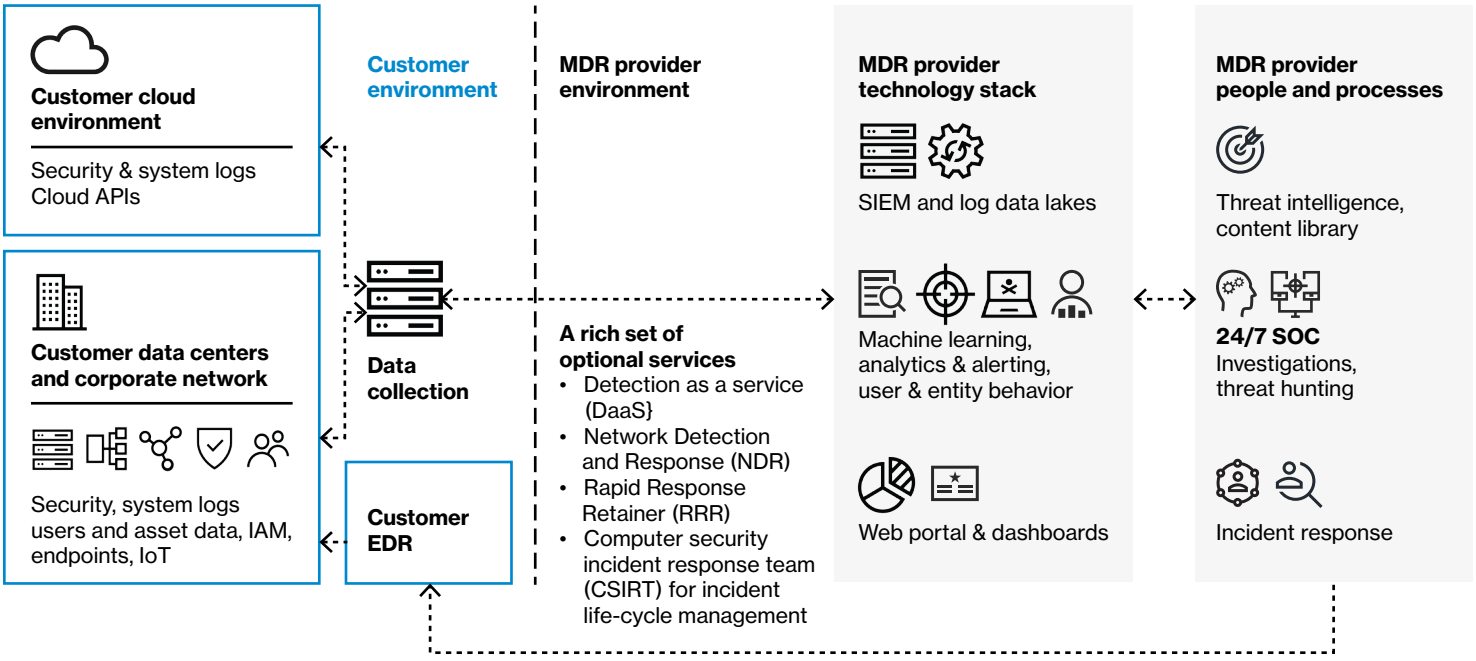

Figure 2: A typical MDR architecture

Recommendation 8: MDR business model and subscription options

Managing the cost of an MDR service is one of the most important considerations for any CISO. MDR vendors use different business models for their service offerings based on:

- Number of endpoints
- Number of users
- Log volume

Explore business model options with your MDR service provider. Find out whether it supports more than one business model and whether those models support your business and long-term goals.

High-level MDR architecture

MDR service architecture should be flexible enough to fit into your environment without causing significant changes to your infrastructure. Figure 2 shows a typical architecture to help you get started.

Fundamentally, the architecture should show clear demarcation points between your environment and MDR service provider environment, as well as how different components of the MDR service work together.

Summary

We know that MDR is a crowded market and it's not easy for you to choose a service provider that could meet your needs. This white paper describes the essential components of an MDR service and provides recommendations to help you navigate through available options and find an appropriate partner to help you achieve your business goals. While technologies and tools will definitely change over time, your main consideration should be the experience and capabilities of your MDR service provider, coupled with the flexibility of optional services and a governance model that enables continuous improvement.

About Verizon Security Solutions

Verizon cybersecurity helps organizations achieve their business objectives and transformational goals with confidence. Our Managed Detection and Response service can help you implement a risk-driven investigation and response program that's continually tuned to meet your needs. Learn more at verizon.com/business/products/security/managed-detection-response-services/managed-detection-and-response/

verizon

1 Rafeeq Rehman, Cybersecurity Arm Wrestling: Winning the Perpetual Fight against Crime by Building a Modern Security Operations Center (SOC), independently published, April 2021.

2 Bruce Shneier, Secrets and Lies: Digital Security in a Networked World, John Wiley and Sons, 2000.